现代数学基础丛书 25

有限群导引

上册

（第二版）

徐明曜 著

科学出版社
www.sciencep.com

(O—1066.0103)


ISBN 978-7-03-007119-4
9 787030 071194
01 >

销售分类建议：高等数学

定 价：36.00 元

现代数学基础丛书 25

有限群导引

上册

（第二版）

徐明曜 著

科学出版社
北京

内 容 简 介

本书分上下册出版. 上册包括前六章和一个附录，可作为综合大学和师范院校数学、物理和化学专业高年级学生的教材，主要内容是，群论的基本概念，群在集合上的作用及其应用，群的构造理论，幂零群和 p-群，可解群和有限群表示论等.

本书用尽量少的篇幅介绍有限群论的基本知识和方法，为了应用特别突出方法，本书包含相当数量的习题. 书末还有解答和提示.

本书适于大学数学、物理、化学高年级学生、研究生、教师和有关科技工作者阅读.

图书在版编目(CIP)数据

有限群导引(上)/徐明曜著. —北京:科学出版社,1999. 3
(现代数学基础丛书;25)
ISBN 978-7-03-007119-4

Ⅰ. 有… Ⅱ. 徐… Ⅲ. 有限群 Ⅳ. 0152. 1

中国版本图书馆 CIP 数据核字(98)第 34282 号

责任印制:安春生/封面设计:黄华斌 陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码: 100717
http://www.sciencep.com
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
1987 年 12 月第 一 版 开本:B5(720×1000)
1999 年 3 月第 二 版 印张:19
2007 年 1 月第四次印刷 字数:242 000
印数:7 401—9 400
定价:36. 00 元
(如有印装质量问题,我社负责调换〈环伟〉)

上册第二版前言

自本书上册于1987年由科学出版社出版以来，已经过去了11年．它作为多所高校数学系研究生和高年级本科生的教材得到了广泛的使用．因此初版印刷的三千册早已售完．另一方面，由于作者方面的原因，本书下册一直未能交稿付印．在这11年间，作者不断收到读者来信询问下册何时出版，以及要求购买早已售缺的上册，这对我们是很大的鞭策和鼓励．现在，在科学出版社的帮助下，终于完成了下册的出版工作，并借此机会重印上册，以飨读者．我们谨对关心本书的学术界朋友和广大读者，以及科学出版社的同志们表示衷心的感谢．

根据使用的情况，我们认为上册的选材和难度等都是比较适当的．再版时拟基本维持原状，在前五章中除改正了原书中的印刷错误外，只作了很少的改动．如对个别定理的证明给了简化等．但是在第VI章中则作了较大的改动．我们根据使用本书的读者多为研究生的实际情况，对常表示的叙述改用模的语言，加入了群代数、半单代数的结构等内容．这可使读者能更深入地理解常表示的实质．另外，“指标”一词按我国数学界的通常叫法改为“特征标”．

上册的部分修改和计算机排版工作是我在广西大学访问时完成的，班桂宁教授给予了很多帮助，特在此致谢．又，北方交大的冯衍全博士也协助进行第VI章的录入工作，在此一并致谢．

徐明曜

1998年于广西大学

上册第一版前言

在抽象代数课程中我们知道，群是现代代数最基本和最重要的概念之一．它在数学本身以及现代科学技术的很多方面都有广泛的应用．比如在理论物理、量子力学、量子化学、结晶学等方面的应用就是明证．因此，在我们学习了抽象代数课程之后，更深入地研究群的理论是很有必要的．

在群论的众多分支中，有限群论无论从理论本身还是从实际应用来说都占据着更为突出的地位．同时，它也是近年来研究最多、最活跃的一个数学分支．最近 20 多年来，经过很多数学家的努力，在有限群中取得了一连串的突破，并终于在 1981 年解决了著名的有限单群分类问题．这项重大的科学成果的得来是很不容易的．如果从 1832 年 Galois 证明交错群 A_5 是单群算起，整整经历了 150 年．参加这项工作的数学家前后共达几百人．为了证明单群分类定理，即有限单群共有 18 个无限族和 26 个零散单群，人们使用了抽象群论的、表示论的 (包括常表示和模表示) 、几何的以及组合论和图论的方法，在杂志上发表了数千页以至上万页的论文．这些论文的总体就构成了单群分类定理的证明．当然人们希望能有一个完整的证明，但在今天看来，要写出这样的证明还需要一定的时间．关于这方面的详细情况，读者可参看 D. Gorenstein 的专著 “Finite Simple Groups” 一书． (Plenum Press, New York, 1982.)

由于这项重大的成果，在数学界中形成了 “有限群热”, 很多学数学甚至学物理的大学生和研究生都想学一点有限群的知识．

从国内来看，不只综合性大学数学系纷纷开设有限群课程，很多师范院校也开了这门课. 本书就是作者 1981–1983 年间在北京大学数学系为大学生和研究生开设有限群课时所编写的讲义. 这个讲义作者前后使用了四次，进行了三次较大的修改. 外校也有一些同志使用这个教材，并提出了不少宝贵的意见和建议.

本书分为上、下两册. 上册包括前六章和一个附录，可作为综合大学或师范学院数学专业本科高年级同学 (已学过抽象代数) 一个学期的选修课的教材. 根据作者的实践，在 54 课时 (每周 3 课时，共 18 周) 的时间中，约可讲完六章中的五章. 只对抽象群感兴趣的教师如感到时间不够可只讲前五章，第 VI 章留给学生自己阅读. 也可以在讲完前三章之后，后面的三章只选讲前面的几节，剩下的材料供学生阅读. 附录中的所谓“研究题”是供大学生做毕业论文时参考用的. 它们或者是较难的习题，或者是一个小的专题，里面包含一些未解决的问题或进一步研究的方向，学完了上册的大学生就可以在这些题目上试试自己的能力. 对于这些研究题，通常我们只指出参考文献，有的也给出解决它的较详细的提示.

本书的下册主要是供研究生用的，其中第 VII–XI 章是有限群的基本知识，对于并非专攻有限群的研究生来说，学习这几章也是有必要的. 但是从第 XII 章起，则是比较专门的材料，它们的选择大部分出自作者个人的兴趣. 但是作者认为在单群分类问题解决之后，它们仍然是可以研究的有意义的课题. 下册如作为研究生一个学期的群论课的教材，前五章是一定要讲的，后面则可由教师随意选讲一部分. 当然全书也可供自学者使用. 读者只要扎实地学完了前 11 章，就能够接触有限群的现代文献，并开始对某些问题进行独立的研究. 从作者的教学实践来看，这点是可以做到的.

还有几点是需要向读者说明的.

1. 本书是作为教材而编写的，目的是用尽量少的篇幅介绍有限群论的基本知识和基本方法，特别是要突出方法. 因此从知识上并不追求完全，相当多的内容是为了介绍方法而写入的.

2. 阅读本书之前应该学过抽象代数课程. 比如读过 N. Jacobson 的 “Basic Algebra I” 的前两章并做过其中大部分习题. 我们劝告那些没有学过抽象代数或者抽象代数训练不够的人不要企图阅读本书. 如果一定要阅读, 势必事倍功半. 基于这种考虑, 第 I 章中多数定理的证明被省略了. 但是这一章还必须仔细阅读, 因为其中补充了很多在抽象代数课程中并不重要但对有限群论具有基本意义的东西.

3. 由于读者都受过较充分的抽象代数的训练, 在本书中定理的证明写得比较简短, 常给读者留有思考的余地. 这样读起来可能会感到吃力, 但对训练推理能力以及将来阅读文献都会有一定的帮助.

4. 本书中的习题是不可不做的, 它们是本书重要的组成部分. 这些习题难易程度不等, 对于稍难一些的题目在书末都附有提示.

5. 我们叙述定义、定理等是依章节统一编号. 在引述前面的结果时, 如果是在本章中, 则不指明所属的章; 如果是在前面各章, 则用罗马数字表明章号. 例如, “定理 2.3” 是指本章中的定理 2.3, 而 “II,3.11” 是指第 II 章的定理 3.11.

编写本书主要参考了以下三本书:

1. B. Huppert, Endliche Gruppen I, Springer-Verlag, 1967.

2. H. Kurzweil, Endliche Gruppen, Springer-Verlag, 1977.

3. D. Gorenstein, Finite Groups, Harper & Row Publishers, New York, 1980.

Huppert 的书是有限群论的一部巨著, 也是搞有限群论的人必备的参考书. 目前这本书的第 II, III 两卷也已经出版, 并加进了合作者 N. Blackburn. 后两卷是用英文写的, 三卷合在一起有近两千页的篇幅. 后两卷是

4. B. Huppert and N. Blackburn, Finite Groups II, III, Springer-Verlag, 1982.

中文的参考书有以下几种:

5. 张远达, 有限群构造, 科学出版社, 1982.

6. 陈重穆，有限群论基础，重庆出版社， 1983.
7. M. Hall 著，裘光明译，群论，科学出版社， 1981.

最后，我要感谢我的导师段学复教授，他给作者很多帮助和鼓励. 此外，我的同事刘力前同志，曾经参加编写 1981 年版本讲义的第七、八两章；河北大学邵惠伯同志、杭州大学姜豪同志、湖南益阳师专陈进之同志以及我校研究生张继平、张来武等同志都对本书提了很多宝贵的修改意见，特在此一并致谢.

徐明曜

1986 年于北京大学

目　录

第 I 章

群论的基本概念

本章是对抽象代数课程中已经学过的群论的基本概念进行复习和补充. 因此, 多数结果不再给出证明.

§1. 群和子群

§1.1 群的定义

定义一个群有多种不同的方式.

定义 1.1 称非空集合 G 为一个 *群*, 如果在 G 中定义了一个二元运算, 叫做乘法, 它满足

(1) *结合律*: $(ab)c = a(bc)$, $a, b, c \in G$;

(2) 存在 *单位元素*: 存在 $1 \in G$, 使对任意的 $a \in G$, 恒有

$$1a = a1 = a;$$

(3) 存在 *逆元素*: 对任意的 $a \in G$, 存在 $a^{-1} \in G$, 使得

$$aa^{-1} = a^{-1}a = 1.$$

上述条件 (2), (3) 可以分别减弱为

(2′) 存在左 (右) 单位元素: 存在 $1 \in G$, 使对任意的 $a \in G$, 有 $1a = a$ $(a1 = a)$;

(3′) 存在左 (右) 逆元素: 对任意的 $a \in G$, 存在 $a^{-1} \in G$, 使得 $a^{-1}a = 1$ $(aa^{-1} = 1)$.

即，条件 (1), (2′) 和 (3′) 亦可定义一个群.

定义 1.2 称非空集合 G 为一个群，如果在 G 中定义了一个二元运算，叫做乘法. 它满足

(1) 结合律： $(ab)c = a(bc)$, $a, b, c \in G$;

(4) 对任意的 $a, b \in G$, 存在 $x, y \in G$, 满足 $ax = b$ 和 $ya = b$.

定义 1.1 和定义 1.2 是等价的.

在任一群 G 中，还成立下述运算规律：

(5)*消去律*: 对任意的 $a, b, c \in G$ 成立

$$ac = bc \Rightarrow a = b$$

和

$$ca = cb \Rightarrow a = b.$$

一般来说，条件 (1) 和 (5) 不足以定义一个群. 例如全体正整数集合对于加法就满足条件 (1) 和 (5), 但它不是群. 可是我们有下面的结论：

定理 1.3 *有限非空集合 G 是群，如果 G 中定义了一个二元运算，满足条件 (1) 和 (5).*

定义 1.4 如果群 G 满足

(6) *交换律*: $ab = ba$, $a, b \in G$, 则称 G 为 *交换群* 或 Abel*群*.

对于以上给出的群的定义，请读者自已检查是否熟悉下列事项的证明：

(1) 由单位元素的存在性推出它的唯一性；

(2) 由逆元素的存在性推出它的唯一性；

(3) 证明条件 (1), (2), (3) 和 (1), (2′), (3′) 的等价性；

(4) 证明定义 1.1 和定义 1.2 的等价性；

(5) 证明定理 1.3;

(6) 由结合律 (1) 推出下面的 *广义结合律*:

(1′) 广义结合律：对于任意有限多个元素 $a_1, a_2, \cdots, a_n \in G$，乘积 $a_1a_2\cdots a_n$ 的任何一种"有意义的加括号方式"[1] 都得出相同的值，因而上述乘积是有意义的.

(7) 在交换群 G 中，乘积 $a_1a_2\cdots a_n$ 的诸因子任意交换次序，其值不变.

注 1.5 (1) 定义一个群还有很多其他的方式, 例如可见 M. Hall 的《群论》(中译本) §1.3.

(2) 如果定义 1.1 中把 (2′), (3′) 两条改为有左单位元素和右逆元素，则 G 不一定是一个群，可参看研究题 1.

下面对我们使用的符号做些说明：我们用大写拉丁字母 $G, H, K, A, B, \cdots$ 表示群或集合，小写拉丁字母 $a, b, c, \cdots$ 表示它的元素；以 1 表示群的单位元素以及仅由单位元素组成的子群，对二者不加区别，读者可从上下文来判断 1 究竟代表单位元素还是单位子群，以 $|G|$ 表示集合 G 的势. 如果 G 是群，则 $|G|$ 叫群的阶. 又，称 G 为有限群，如果 $|G|$ 是有限数，否则叫做无限群.

由广义结合律 (1′), 任意有限多个元素的乘积 $a_1a_2\cdots a_n$ 是有意义的. 特别地，我们可以规定群 G 中元素 a 的整数次方幂如下：设 n 为正整数，则

$$a^n = \underbrace{aa\cdots a}_{n\text{ 个}},\ a^0 = 1,\ a^{-n} = (a^{-1})^n.$$

显然有

$$a^m a^n = a^{m+n},\ m, n\text{是整数}.$$

又，对于乘积的逆，有下列法则：

命题 1.6 设 G 是群，$a_1, a_2, \cdots, a_n \in G$, 则

$$(a_1a_2\cdots a_n)^{-1} = a_n^{-1}\cdots a_2^{-1}a_1^{-1}.$$

[1] 因为群的乘法是二元运算，根据定义，只有两个元素的乘积才有意义，多个元素的乘积必须通过逐步作两个元素的乘积来实现. 所谓"有意义的加括号方式"指的就是给定的一种确定的运算次序. 例如对乘积 $abcde$, 我们称 $((ab)c)(de)$, $((a(bc))d)e, \cdots$ 等为"有意义的加括号方式"，但 $((abc)d)e$, $(ab)(cd)e, \cdots$ 等则不是.

§1.2 子群

设 G 是群， H,K 是 G 的子集，规定 H,K 的乘积为

$$HK = \{hk \mid h \in H, k \in K\}.$$

如果 $K = \{a\}$，仅由一个元素 a 组成，则简记为 $H\{a\} = Ha$; 类似地有 aH 等. 我们还规定

$$H^{-1} = \{h^{-1} \mid h \in H\}.$$

很明显，子集的乘法也满足结合律，因而也可以定义子集 H 的正整数次幂 H^n，并且对子集的乘法也成立命题 1.6.

定义 1.7 称群 G 的非空子集 H 为 G 的 *子群*，如果 $H^2 \subseteq H$, $H^{-1} \subseteq H$. 这时记作 $H \leq G$.

事实上，易验证如果 H 是 G 的子群，则必有 $H^2 = H$, $H^{-1} = H$，并且 $1 \in H$. 显然，任何群 G 都有二子群 G 和 1，叫做 G 的 *平凡子群*.

命题 1.8 *设 G 是群， $H \subseteq G$; 则下列命题等价:*

(1) $H \leq G$;

(2) 对任意的 $a,b \in H$，恒有 $ab \in H$ 和 $a^{-1} \in H$;

(3) 对任意的 $a,b \in H$，恒有 $ab^{-1} \in H$(或 $a^{-1}b \in H$).

命题 1.9 *设 G 是群， $H \subseteq G$, $|H|$ 是有限数，则*

$$H \leq G \iff H^2 \subseteq H.$$

若干个子群的交仍为子群，即我们有

定理 1.10 *设 G 是群. 若 $H_i \leq G$, $i \in I$, I 是某个指标集，则 $\bigcap_{i\in I} H_i \leq G$.*

一般来说若干子群的并不是子群，但我们有下述概念:

定义 1.11 设 G 是群, $M \subseteq G$ (允许 $M = \varnothing$), 则称 G 的所有包含 M 的子群的交为 *由 M 生成的子群*, 记作 $\langle M \rangle$.

容易看出, $\langle M \rangle = \{1, a_1a_2\cdots a_n \mid a_i \in M \cup M^{-1}, n = 1, 2, \cdots\}$.

如果 $\langle M \rangle = G$, 我们称 M 为 G 的一个 *生成系*, 或称 G 由 M 生成. 仅由一个元素 a 生成的群 $G = \langle a \rangle$ 叫做 *循环群*. 可由有限多个元素生成的群叫做 *有限生成群*. 有限群当然都是有限生成群.

对于群 G 中任意元素 a, 我们称 $\langle a \rangle$ 的阶为 *元素 a 的阶*, 记作 $o(a)$, 即 $o(a) = |\langle a \rangle|$. 由此定义, $o(a)$ 是满足 $a^n = 1$ 的最小的正整数 n, 而如果这样的正整数 n 不存在, 则 $o(a) = \infty$.

下面的结论是十分重要的.

定理 1.12 设 G 是群, $H \le G, K \le G$, 则

$$HK \le G \iff HK = KH.$$

证 $\Rightarrow$: 由 $HK \le G$ 有 $(HK)^{-1} = HK$, 即 $K^{-1}H^{-1} = HK$. 又由 $H \le G, K \le G$, 有 $H^{-1} = H, K^{-1} = K$, 于是 $KH = HK$.

$\Leftarrow$: 由 $HK = KH$ 可得 $(HK)^2 = HKHK = HHKK = HK$, $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$, 由定义 1.7 即得 $HK \le G$. □

§1.3 子群的陪集

定义 1.13 设 $H \le G, a \in G$. 称形如 $aH(Ha)$ 的子集为 H 的一个 *左 (右) 陪集*. 容易验证 $aH = bH \iff a^{-1}b \in H$. 类似地有 $Ha = Hb \iff ab^{-1} \in H$.

命题 1.14 设 $H \le G, a, b \in G$, 则

(1) $|aH| = |bH|$;

(2) $aH \cap bH \neq \varnothing \Rightarrow aH = bH$.

于是, G 可表成 H 的互不相交的左陪集的并:

$$G = a_1H \cup a_2H \cup \cdots \cup a_nH,$$

元素 $\{a_1, a_2, \cdots, a_n\}$ 叫做 H 在 G 中的一个 (左) 陪集代表系. H 的不同左陪集的个数 n (不一定有限) 叫做 H 在 G 中的 **指数**, 记作 $|G:H|$.

同样的结论对于右陪集也成立, 并且 H 在 G 中的左、右陪集个数相等, 都是 $|G:H|$.

下面的定理对于有限群具有基本的重要性.

定理 1.15 (Lagrange) *设 G 是有限群, $H \le G$, 则 $|G| = |H||G:H|$.*

由此定理, 在有限群 G 中, 子群的阶是群阶的因子. 而且还可推出, G 中任一元素 a 的阶 $o(a)$ 也是 $|G|$ 的因子. 这因为 $o(a) = |\langle a\rangle|$, 而 $\langle a\rangle \le G$.

定义 1.16 称群 G 为 *周期群*, 如果 G 的每个元素都是有限阶的. 又如果 G 中所有元素的阶存在最小公倍数 m, 则称 m 为 G 的 *方次数*, 记作 $\exp G = m$.

显然, 有限群是周期群, 存在方次数, 并且 $\exp G \,\big|\, |G|$.

定理 1.17 *设 G 是群. 如果 $\exp G = 2$, 则 G 是交换群.*

证 对任意的 $a, b \in G$, 由 $1 = (ab)^2 = a^2b^2$ 得 $abab = aabb$, 左乘 a^{-1}, 右乘 b^{-1}, 即得 $ab = ba$. □

定理 1.18 *设 G 是群, H 和 K 是 G 的有限子群, 则*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

证 因为群 G 的子集 HK 是由形如 $Hk(k \in K)$ 的 H 的右陪集的并组成, 每个右陪集含有 $|H|$ 个元素, 故为证明上式只须证 HK 中含有 $|K : H \cap K|$ 个 H 的右陪集. 由

$$Hk_1 = Hk_2 \iff k_1k_2^{-1} \in H,$$

注意到 $k_1k_2^{-1} \in K$, 故

$$\begin{aligned} Hk_1 = Hk_2 \quad &\Longleftrightarrow \quad k_1k_2^{-1} \in H \cap K \\ &\Longleftrightarrow \quad (H \cap K)k_1 = (H \cap K)k_2. \end{aligned}$$

因此 HK 中包含 H 的右陪集个数等于 $H \cap K$ 在 K 中的指数 $|K : H \cap K|$, 得证. □

命题 1.19 设 G 是有限群, $H \leq G, K \leq G$, 则
(1) $|\langle H, K\rangle : H| \geq |K : H \cap K|$;
(2) $|G : H \cap K| \leq |G : H||G : K|$;
(3) 若 $|G : H|$ 和 $|G : K|$ 互素, 则

$$|G : H \cap K| = |G : H||G : K|,$$

并且此时有 $G = HK$.

证 (1) 由上定理的证明中我们已经看到, 子集 HK 中包含 H 的右陪集个数 (姑且记作 $|HK : H|$) 等于 $|K : H \cap K|$. 因为 $\langle H, K\rangle \supseteq HK$, 自然有

$$|\langle H, K\rangle : H| \geq |HK : H| = |K : H \cap K|.$$

(2) 因为

$$|G : H \cap K| = |G : K||K : H \cap K|,$$

由 $|G : H| \geq |\langle H, K\rangle : H|$ 及 (1), 有 $|G : H| \geq |K : H \cap K|$, 于是有

$$|G : H \cap K| \leq |G : H||G : K|.$$

(3) 由 Lagrange 定理, $|G : H|$ 和 $|G : K|$ 都是 $|G : H \cap K|$ 的因子. 又因 $|G : H|$ 和 $|G : K|$ 互素, 有

$$|G : H||G : K| \mid |G : H \cap K|.$$

再由 (2) 即得

$$|G : H \cap K| = |G : H||G : K|.$$

但另一方面，

$$|G:H\cap K|=|G:K||K:H\cap K|=|G:K||HK:H|,$$

由此推出 $|G:H|=|HK:H|$，于是 $G=HK$. □

§1.4 共轭

设 G 是群， $a,g\in G$，我们规定

$$a^g=g^{-1}ag,$$

并称 a^g 为 a 在 g 之下的 **共轭变形**. 对于 G 的子群或子集 H，我们同样规定

$$H^g=g^{-1}Hg,$$

也叫做 H 在 g 下的共轭变形. 容易验证下面的结论：

命题 1.20 *共轭变形运算满足*

(1) $a^{gh}=(a^g)^h$;

(2) $(ab)^g=a^gb^g$;

(3) $(a^g)^{-1}=(a^{-1})^g$.

定义 1.21 称群 G 的元素 a, b (或子群或子集 H,K) 在 G 中**共轭**，如果存在元素 $g\in G$，使 $a^g=b$ (或 $H^g=K$).

命题 1.22 *(在元素间，子群间或子集间的) 共轭关系是等价关系.*

于是，群 G 的所有元素依共轭关系可分为若干互不相交的等价类 (叫做 **共轭类**) $C_1=\{1\},C_2,\cdots,C_k$，并且

$$G=C_1\cup C_2\cup\cdots\cup C_k.$$

由此又有

$$|G|=|C_1|+|C_2|+\cdots+|C_k|,$$

叫做 G 的 **类方程**，而 k 叫做 G 的 **类数**. 共轭类 C_i 包含元素的个数 $|C_i|$ 叫做 C_i 的 **长度**.

为了研究共轭类的长度，我们规定

定义 1.23 设 G 是群， H 是 G 的子集， $g \in G$. 若 $H^g = H$, 则称元素 g 正规化 H, 而称 G 中所有正规化 H 的元素的集合

$$N_G(H) = \{g \in G \mid H^g = H\}$$

为 H 在 G 中的 正规化子. 又若元素 g 满足对所有 $h \in H$ 恒有 $h^g = h$, 则称元素 g中心化H, 而称 G 中所有中心化 H 的元素的集合

$$C_G(H) = \{g \in G \mid h^g = h,\ \forall h \in H\}$$

为 H 在 G 中的 中心化子.

规定 $Z(G) = C_G(G)$, 并称之为群 G 的 中心.

易验证, 对于任意子集 H, $N_G(H)$ 和 $C_G(H)$ 都是 G 的子群. 并且若 $H \le G$, 则 $H \le N_G(H)$. 如果 H 是单元素集 $\{a\}$, 则 $N_G(H)$ 和 $C_G(H)$ 分别记作 $N_G(a)$ 和 $C_G(a)$, 这时有 $C_G(a) = N_G(a)$.

定理 1.24 G 中元素 a 所属的共轭类 C 的长度 $|C| = |G : C_G(a)|$, 因此， $|C|$ 是 $|G|$ 的因子. 类似地, 子群 (或子集) H 的共轭子群 (或共轭子集) 的个数为 $|G : N_G(H)|$, 也是 $|G|$ 的因子.

§1.5 双陪集

定义 1.25 设 H, K 是有限群 G 的子群，我们称形如 HaK, $a \in G$, 的子集为 G 关于子群 H 和 K 的一个 双陪集.

类似于陪集，我们有

命题 1.26 对于双陪集成立

$$HaK \cap HbK \neq \varnothing \Rightarrow HaK = HbK.$$

于是， G 可表成互不相交的若干双陪集的并:

$$G = Ha_1K \cup Ha_2K \cup \cdots \cup Ha_sK.$$

证 设 $hak = h'bk' \in HaK \cap HbK$, $h, h' \in H$, $k, k' \in K$. 则 $a = (h^{-1}h')b(k'k^{-1})$, 其中 $h^{-1}h' \in H$, $k'k^{-1} \in K$. 于是有

$$HaK = H(h^{-1}h')b(k'k^{-1})K = HbK.$$

□

定理 1.27 *任一双陪集 HaK 可表成若干 H 的右陪集 (或 K 的若干左陪集) 的并. 它包含 H 的右陪集的个数为 $|K : H^a \cap K|$, 而包含 K 的左陪集的个数为 $|H^a : H^a \cap K|$.*

证 我们只证明关于右陪集的结论.

假定 $g \in HaK$, 则 $Hg \subseteq H(HaK) = HaK$. 因此 HaK 由若干个 H 的右陪集的并组成. 设 HaK 包含 n 个 H 的右陪集, 则

$$n = |HaK|/|H|.$$

又显然有

$$|HaK| = |a^{-1}HaK| = |H^aK|.$$

由定理 1.18,

$$|H^aK| = \frac{|H^a||K|}{|H^a \cap K|} = \frac{|H||K|}{|H^a \cap K|},$$

于是

$$n = \frac{|H||K|}{|H^a \cap K||H|} = \frac{|K|}{|H^a \cap K|} = |K : H^a \cap K|.$$

□

§1.6 同态和同构

我们假定读者已经熟知群的同态和同构的概念. 下面的简短说明只是为了固定符号的使用.

我们称映射 $\alpha : G \to G_1$ 为群 G 到 G_1 的一个同态映射, 如果

$$(ab)^\alpha = a^\alpha b^\alpha, \ \forall a, b \in G.$$

如果 α 是满 (单) 射，则称为满 (单) 同态；而如果 α 是双射，即一一映射，则称 α 为 G 到 G_1 的同构映射. 这时称群 G 和 G_1 同构，记作 $G \cong G_1$.

群 G 到自身的同态及同构具有重要的意义，我们称之为群 G 的自同态和自同构. 在本书中，我们以 $\mathrm{End}(G)$ 表示 G 的全体自同态组成的集合，而以 $\mathrm{Aut}(G)$ 表示 G 的全体自同构组成的集合. 对于映射的乘法， $\mathrm{End}(G)$ 组成一个有单位元的半群，而 $\mathrm{Aut}(G)$ 组成一个群，叫做 G 的自同构群.

对于 $g \in G$, 由 $g^{\sigma(g)} = a^g$ 规定的映射 $\sigma(g) : G \to G$ 是 G 的一个自同构，叫做由 g 诱导出的 G 的内自同构, G 的全体内自同构集合 $\mathrm{Inn}(G)$ 是 $\mathrm{Aut}(G)$ 的一个子群，并且映射 $\sigma : g \mapsto \sigma(g)$ 是 G 到 $\mathrm{Inn}(G)$ 的一个满同态.

习 题

1. 设 G 是群， $a, b \in G$. 则 $o(a) = o(a^{-1})$, $o(ab) = o(ba)$.

2. 设 G 是群， $g \in G$, $o(g) = n$. 则 $o(g^m) = n/(m, n)$.

3. 设 $H \leq G$, $g \in G$. 若 $o(g) = n$, 且 $g^m \in H$, $(n, m) = 1$, 则 $g \in H$.

4. 设 G 是群， $g_1, g_2 \in G$. 若 $o(g_1) = n_1$, $o(g_2) = n_2$, $(n_1, n_2) = 1$, 且 $g_1g_2 = g_2g_1$, 则 $o(g_1g_2) = n_1n_2$. 并举例说明如果 $g_1g_2 \neq g_2g_1$, 则无此结论.

5. 设 G 是群, $g \in G$. 若 $o(g) = n_1n_2$, $(n_1, n_2) = 1$, 则存在 $g_1, g_2 \in G$, 使 $g = g_1g_2 = g_2g_1$, 并且 $o(g_1) = n_1$, $o(g_2) = n_2$. 证明 g_1, g_2 被这些条件所唯一决定.

6. 若群 G 只有一个 2 阶元素 a, 则 $a \in Z(G)$.

7. 设 p, q 是素数，且 $p < q$, 则 pq 阶群有唯一的 q 阶子群 (证明时不要用 Sylow 定理).

8. 设 $H \leq G$, $K \leq G$, 则 $H \cup K \leq G \iff H \leq K$ 或 $K \leq H$.

9. 设 $H \leq G$, $K \leq G$, $a, b \in G$. 若 $Ha = Kb$, 则 $H = K$.

10. 设 $H < G$, 且 $|G : N_G(H)| = 2$, 则对任意的 $x \in G$ 有 $HH^x = H^xH$.

11. 设 $H < G$, 且 $H_1, \cdots, H_n$ 是 H 在 G 中的全部共轭子群 (排列成任意次序), 则

$$\langle H_1, \cdots, H_n \rangle = H_1 \cdots H_n.$$

12. 设 $|G|=n$, $a_1,a_2,\cdots,a_n$ 是群 G 的 n 个元素，不一定互不相同，则存在整数 i,j, $1\le i\le j\le n$ 使 $a_ia_{i+1}\cdots a_j=1$.

13. 设 G 是群. 令 $K=\{a_1,a_2,\cdots,a_n\}\subseteq G$ 且 $1\notin K^2$, 则在 n^2 个乘积 a_ia_j 中至多有 $\frac{n(n-1)}{2}$ 个属于 K.

14. 设 A,B,C 皆为 G 之子群. 若 $B\le A$, 则

$$|A:B|\ge|(C\cap A):(C\cap B)|.$$

15. 设 A,B,C 为 G 之子群，并且 $A\le C$, 则

$$AB\cap C=A(B\cap C).$$

注：对于熟悉格的概念的读者，上式即格中之模律, 因 AB 不一定是 G 的子群，所以它不能看成是 G 的子群格中的等式. 但若 A,B,C 均为 G 之正规子群，则上式即说明任一群之正规子群组成的格为模格.

16. 设 A,B,C 为群 G 之子群，并且 $A\le B$. 如果 $A\cap C=B\cap C$, $AC=BC$, 则必有 $A=B$.

17. 设 $A,B\le G$, 则

$$\langle A,B\rangle=\bigcup_{i=1}^{\infty}(AB)^i.$$

又若 G 为有限群，则存在正整数 n 使 $\langle A,B\rangle=(AB)^n$.

18. 设 $a,b,x,y\in G$. 若 a 与 x 共轭， b 与 y 共轭，问 ab 是否与 xy 共轭？若又加条件 $ab=ba, xy=yx$ 呢？或再加条件 $(o(a),o(b))=1$ 呢？试举例说明之.

19. 证明除平凡子群外无其它子群的群必为素数阶循环群.

§2. 正规子群和商群

§2.1 正规子群和商群

定义 2.1 称群 G 的子群 N 为 G 的 *正规子群*, 如果 $N^g\subseteq N$, $\forall g\in G$. 记作 $N\trianglelefteq G$.

命题 2.2 *设 G 是群，则下列事项等价：*

(1) $N\trianglelefteq G$;

(2) $N^g=N$, $\forall g\in G$ (*因此正规子群也叫自共轭子群*);

(3) $N_G(N)=G$;

(4) 若 $n\in N$, 则 n 所属的 G 的共轭元素类 $C(n)\subseteq N$, 即 N 由 G 的若干整个的共轭类组成;

(5) $Ng=gN$, $\forall g\in G$;

(6) N 在 G 中的每个左陪集都是一个右陪集.

根据 (6), N 的左，右陪集的集合是重合的，因此，对正规子群我们可只讲陪集，而不区分左右.

显然，交换群的所有子群皆为正规子群. 又，任一群 G 都至少有两个正规子群： G 和 1, 叫做 *平凡的* 正规子群.

定义 2.3 只有平凡正规子群的群叫做 *单群*.

因为交换群的每个子群都是正规子群，由上节习题 19, 交换单群只有素数阶循环群. 而非交换单群则有十分复杂的情形. 事实上，决定所有有限非交换单群多年来一直是有限群论的核心问题.

下面的事实是常用到的.

命题 2.4 设 $N_1, N_2, \ldots, N_s$ 是群 G 的正规子群，则 $\bigcap_{i=1}^{s} N_i$ 和 $\langle N_1, N_2, \ldots, N_s\rangle$ 也是 G 的正规子群.

命题 2.5 设 $N\trianglelefteq G, H\leq G$, 则 $\langle N, H\rangle = NH = HN$.

定义 2.6 设 G 是群， $M\subseteq G$, 称

$$M^G = \langle m^g \mid m\in M, g\in G\rangle$$

为 M 在 G 中的 *正规闭包*, M^G 是 G 的包含 M 的最小的正规子群.

下面设 $N\trianglelefteq G$. 我们研究 N 的所有陪集的集合 $\overline{G}=\{Ng \mid g\in G\}$. 定义 $\overline{G}$ 中的乘法为群子集的乘法，即

$$(Ng)(Nh) = N(gN)h = N(Ng)h = N^2gh = Ngh, \qquad (*)$$

则我们有

定理 2.7 $\overline{G}$ 对乘法 $(*)$ 封闭，并且成为一个群，叫做 G 对 N 的 *商群*, 记作 $\overline{G}=G/N$.

§2.2 同态定理和同构定理

设 $\alpha: G \to H$ 是群同态映射，则

$$\operatorname{Ker}\alpha = \{g \in G \mid g^\alpha = 1\}$$

叫做同态 α 的 **核**, 而

$$G^\alpha = \{g^\alpha \mid g \in G\}$$

叫做同态 α 的 **像集**, 容易验证 $\operatorname{Ker}\alpha \trianglelefteq G$, 而 $G^\alpha \leq H$.

下面的定理是基本的.

定理 2.8 (同态基本定理)

(1) 设 $N \trianglelefteq G$, 则映射 $\nu: g \mapsto Ng$ 是 G 到 G/N 的同态映射, 满足 $\operatorname{Ker}\nu = N$, $G^\nu = G/N$. 这样的 ν 叫做 G 到 G/N 上的自然同态.

(2) 设 $\alpha: G \to H$ 是同态映射, 则 $\operatorname{Ker}\alpha \trianglelefteq G$, 且 $G^\alpha \cong G/\operatorname{Ker}\alpha$.

根据同态基本定理，群的同态像从同构的意义上说就是群对正规子群的商群.

定理 2.9 (第一同构定理) 设 $N \trianglelefteq G$, $M \trianglelefteq G$, 且 $N \leq M$, 则 $M/N \trianglelefteq G/N$, 并且

$$(G/N)/(M/N) \cong G/M.$$

定理 2.10 (第二同构定理) 设 $H \leq G$, $K \trianglelefteq G$, 则 $(H \cap K) \trianglelefteq H$, 且 $HK/K \cong H/(H \cap K)$.

研究群的同态像对于群的构造问题是很重要的. 例如，研究群 G 到域 K 上的 n 阶可逆矩阵群内的同态像，即所谓 G 在域上的矩阵表示，就形成了群论的 (甚至独立于群论的) 一个分支——群表示论. 它在上世纪末和本世纪四十年代得到了决定性的发展，对于有限群的构造的研究起了十分重要的作用.

§2.3 直积

我们已经熟悉两个群 G, H 的 (外) 直积

$$G \times H = \{(g,h) \mid g \in G, h \in G\},$$

其中乘法如下规定:

$$(g,h)(g',h') = (gg', hh'),\ g, g' \in G, h, h' \in H.$$

类似地, 可定义 n 个群 $G_1, \cdots, G_n$ 的 (外) 直积

$$G = G_1 \times G_2 \times \cdots \times G_n.$$

在上述 (外) 直积中, 对于 $i = 1, 2, \cdots, n$, 令

$$H_i = \{(1, \cdots, 1, g_i, 1, \cdots, 1) \mid g_i \in G_i\},$$

其中 g_i 是第 i 个分量, 则显然有 $H_i \cong G_i$, 并且还成立下述事实:

1) $H_i \trianglelefteq G, \forall i$;

2) $G = \langle H_1, H_2, \cdots, H_n \rangle = H_1 H_2 \cdots H_n$;

3) 对 $i \neq j$, H_i 和 H_j 的元素可交换, 即对任意的 $h_i \in H_i$, $h_j \in H_j$, 恒有 $h_i h_j = h_j h_i$;

4) $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = 1, \forall i$;

5) G 的任意元素 h 可表为 $H_1, \cdots, H_n$ 中的元素的乘积, 而且表示方法是唯一的. 即若有

$$h = h_1 \cdots h_n = h_1' \cdots h_n',\ h_1, h_1' \in H_1;\ \cdots;\ h_n, h_n' \in H_n,$$

则必有 $h_1 = h_1', \cdots, h_n = h_n'$.

事实上, 在有限群中用得更多的是所谓 内直积 的概念.

我们称群 G 是子群 H, K 的 (内) 直积, 如果 $G = HK$ 并且映射 $(h,k) \mapsto hk$ 是 $H \times K \to G$ 的同构映射. 这时我们也记成 $G = H \times K$, 即符号与外直积不加区别. 类似地, 可规定群 G 是 n 个子群 $G_1, \cdots, G_n$ 的 (内) 直积的意义.

容易验证, 外直积 $G = G_1 \times \cdots \times G_n$ 也是前面规定的子群 $H_1, \cdots, H_n$ 的内直积, 即 $G = H_1 \times \cdots \times H_n$, 而且对于内直积也成立上面的 1)–5). 更进一步, 我们有下面的

定理 2.11 群 G 是子群 $H_1, \cdots, H_n$ 的 (内) 直积的充要条件是

(1) $H_i \trianglelefteq G$, $i = 1, 2, \cdots n$;

(2) $G = H_1 H_2 \cdots H_n$;

(3) $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = 1$, $i = 1, \cdots, n$.

其中条件 (3) 还可减弱为

(3′) $H_i \cap (H_1 \cdots H_{i-1}) = 1$, $i = 2, \cdots, n$.

即条件 (1), (2), (3′) 也是 $G = H_1 \times \cdots \times H_n$ 的充要条件, 而且我们还有

定理 2.11′ 群 G 是子群 $H_1, \cdots, H_n$ 的 (内) 直积的充要条件是

(1) $H_i \trianglelefteq G$, $i = 1, 2, \cdots, n$;

(2) $G = H_1 H_2 \cdots H_n$;

(4) G 的每个元素 h 表为 $H_1, \cdots, H_n$ 的元素的乘积的表示方法是唯一的, 即若

$$h = h_1 h_2 \cdots h_n = h_1' h_2' \cdots h_n', \ h_i, h_i' \in H_i, \ i = 1, 2, \cdots, n,$$

则 $h_i = h_i'$, $i = 1, \cdots, n$.

条件 (4) 还可减弱为 G 的单位元素 1 的表示法唯一, 即若

$$1 = h_1 h_2 \cdots h_n, \ h_i \in H_i, \ i = 1, \cdots, n,$$

则 $h_1 = h_2 = \cdots = h_n = 1$.

§2.4 特征子群

定义 2.12 称群 G 的子群 H 为 G 的特征子群, 如果 $H^\alpha \subseteq H$, $\forall \alpha \in \mathrm{Aut}(G)$. 这时记作 H char G.

定义 2.13 称群 G 的子群 H 为 G 的全不变子群, 如果 $H^\alpha \subseteq H$, $\forall \alpha \in \mathrm{End}(G)$.

类似地, 正规子群的定义 (定义 2.1) 也可以改述为

定义 2.14 称群 G 的子群 H 为 G 的**正规子群**, 如果 $H^{\alpha} \subseteq H$, $\forall \alpha \in \mathrm{Inn}(G)$.

由 $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G) \subseteq \mathrm{End}(G)$, 有
H 是 G 的全不变子群 $\Longrightarrow$ H 是 G 的特征子群 $\Longrightarrow$ H 是 G 的正规子群.

命题 2.15 (1) K char H, H char $G \Longrightarrow K$ char G;
(2) K char H, $H \trianglelefteq G \Longrightarrow K \trianglelefteq G$.

但一般来说, $K \trianglelefteq H$ 和 $H \trianglelefteq G$ 不能推出 $K \trianglelefteq G$. 请读者举例说明之.

群 G 的平凡子群 G 和 1 显然都是 G 的特征子群和全不变子群. 又, 群 G 的中心 $Z(G)$ 是 G 的特征子群, 但不一定是全不变子群 (见本节末的习题 6).

定义 2.16 称群 G 为**特征单群**, 如果 G 没有非平凡的特征子群.

定理 2.17 *有限特征单群 G 是同构单群的直积.*

证 设 N 是 G 的任一**极小正规子群**, 即 G 的 $\neq 1$ 的正规子群的集合在包含关系之下的极小元素. 则对任一 $\alpha \in \mathrm{Aut}(G)$, N^{α} 显然也是 G 的极小正规子群. 假定 M 是形状为若干 N^{α} 直积的子群中的极大者. 可令

$$M = N_1 \times \cdots \times N_s,$$

其中 $N_i = N^{\alpha_i}$, $\alpha_i \in \mathrm{Aut}(G)$, $i = 1, \cdots, s$. 这时显然有 $M \trianglelefteq G$. 我们断言, M 实际上包含任一 N^{α}, 对 $\alpha \in \mathrm{Aut}(G)$. 这因为若有某个 $N^{\beta} \not\leq M$, $\beta \in \mathrm{Aut}(G)$, 则因 $N^{\beta} \trianglelefteq G$, 推知 $N^{\beta} \cap M \trianglelefteq G$. 由 N^{β} 的极小性必有 $N^{\beta} \cap M = 1$, 于是 $\langle M, N^{\beta} \rangle = M \times N^{\beta} = N_1 \times \cdots \times N_s \times N^{\beta}$, 这与 M 的选取相矛盾. 这样我们证明了 $M = \langle N^{\alpha} \mid \alpha \in \mathrm{Aut}(G) \rangle$, 于是 M char G. 由 G 的特征单性, 又得到

$$G = M = N_1 \times \cdots \times N_s.$$

为完成定理的证明，还须证 N_i 是单群. 若否， N_i 的任一非平凡正规子群也必为直积 $N_1\times\cdots\times N_s=G$ 的正规子群 (参看本节末习题 3), 这与 N_i 是 G 的极小正规子群相矛盾. □

另一方面，我们也能证明，任意有限多个同构单群的直积必为特征单群 (见本章 §7 中的例 7.8 和例 7.9). 这样，如果我们知道了全部的有限单群，则有限特征单群也就全都知道了.

推论 2.18 *有限群 G 的极小正规子群 N 必为同构单群的直积.*

证 首先， N 必为特征单群. 因若有 K char N ，由 $N\trianglelefteq G$ 及命题 2.15(2) 得 $K\trianglelefteq G$. 再由 N 的极小性得 $K=N$ 或 $K=1$. 这样， N 是特征单群. 根据定理 2.17, 即得 N 是同构单群的直积. □

习　题

1. 设 G 是有限群， $N\trianglelefteq G, g\in G$. 若 $(o(g),|G/N|)=1$, 则 $g\in N$.
2. 设 $H\trianglelefteq G$, $(|H|,|G/H|)=1$, 则 H char G.
3. 证明群 A 的正规子群也是直积 $A\times B$ 的正规子群.
4. 证明 $Z(A\times B)=Z(A)\times Z(B)$.
5. 若 $H\le Z(G)$, 则 $H\trianglelefteq G$. 又若 G/H 是循环群，则 G 是交换群.
6. 举例说明 $Z(G)$ 不一定是 G 的全不变子群.
7. 证明 $\mathrm{Inn}(G)\cong G/Z(G)$.
8. 设 $G_1,\cdots,G_n$ 是有限群 G 的正规子群，且 $G=\langle G_1,\cdots,G_n\rangle$. 若对任意的 $i\ne j$, $(|G_i|,|G_j|)=1$, 则
(1) $G=G_1\times\cdots\times G_n$;
(2) $\mathrm{Aut}(G)=\mathrm{Aut}(G_1)\times\cdots\times\mathrm{Aut}(G_n)$.
9. 若 $\mathrm{Aut}(G)=1$, 则 $G=1$ 或 Z_2.
10. 若 $H\le G, K\le G$, 且 $|H|=|K|$, $(|H|,|G:H|)=1$, 则

$$N_H(K)=N_K(H)=H\cap K.$$

11. 设 G 是有限群， $H\le G, N\trianglelefteq G$.
(1) 若 $(|G:N|,|H|)=1$, 则 $H\le N$;

(2) 若 $(|G:H|, |N|) = 1$, 则 $N \leq H$.

12. 设 H 是群 G 的有限指数子群, 则 H 包含一个 G 的正规子群 N, 它在 G 中也有有限指数.

13. 设 S 是群 G 的有限子集, 且 $N_G(S) = G$. 设 $n > 0$ 是一个正整数, 满足 $s^n = 1$, $\forall s \in S$. 则 G 的子群 $\langle S \rangle$ 的每个元素都可表成 G 的不超过 $(n-1)|S|$ 个元素的乘积 (因子可以重复). 特别地, $\langle S \rangle$ 必为有限子群.

14. 设 G 是群, H 是 G 的有限指数子群, 且 $|G:H| = n$. 又设 $z \in Z(G)$, 则 $z^n \in H$.

15. 设 G 是群, $\mathfrak{S} = \{S_i \subseteq G \mid i \in I\}$ 是 G 的一族非空子集, 满足:

(1) $\bigcup_{i \in I} S_i = G$;

(2) 不存在 $i, j \in I$ 使 $S_i \subsetneqq S_j$;

(3) 对任意的 $i, j \in I$, 可找到 $k \in I$ 使 $S_i S_j \subseteq S_k$. 则 $\mathfrak{S}$ 一定是 G 关于某个正规子群的所有陪集的集合.

§3. 群例

由于读者已经学过抽象代数, 本节的目的不是用例子来解释群的概念, 而是罗列经常遇到的一些具体的群例以及它们的性质.

§3.1 由数组成的群

首先对几个基本数系的符号规定如下: 正整数 $\mathbb{N}$, 整数系 $\mathbb{Z}$, 有理数系 $\mathbb{Q}$, 实数系 $\mathbb{R}$, 复数系 $\mathbb{C}$.

例 3.1 $\mathbb{Z}$ 对加法成群 $(\mathbb{Z}, +)$.

例 3.2 任一数域 F 对加法成群 $(F, +)$. 特别地, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ 是群.

例 3.3 任一数域 F 的非零元素集合 $F^{\#}$ 对乘法成群 $(F^{\#}, \cdot)$ 特别地, $(\mathbb{Q}^{\#}, \cdot), (\mathbb{R}^{\#}, \cdot), (\mathbb{C}^{\#}, \cdot)$ 是群.

例 3.4 正有理数集 $\mathbb{Q}^+$ 和正实数集 $\mathbb{R}^+$ 对乘法成群 $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R}^+, \cdot)$.

例 3.5 模为 1 的全体复数对乘法成群 $\mathbb{C}_1$.

例 3.6 设 n 为正整数，n 次单位根的全体对乘法组成群 U_n，并且 $\bigcup_{n=1}^{\infty} U_n = U$ 对乘法也成群. 容易证明，由数组成的所有有限乘法群都是 U 的子群.

例 3.7 整数环 $\mathbb{Z}$ 关于理想 (n) 的同余类环 $\mathbb{Z}_n = \mathbb{Z}/(n)$ 对加法成群 $(\mathbb{Z}_n, +)$.

§3.2 循环群

设 $G = \langle a \rangle$ 是循环群，a 是其生成元. 考虑映射 $\alpha : \mathbb{Z} \to G$，满足 $i^\alpha = a^i, i \in \mathbb{Z}$. 易验证 α 是同态映射，因而 $G \cong \mathbb{Z}/\text{Ker}\ \alpha$，而

$$\text{Ker}\ \alpha = \begin{cases} \{0\}, & o(a) = \infty, \\ \{kn \mid k \in \mathbb{Z}\}, & o(a) = n. \end{cases}$$

故得

定理 3.8 *无限循环群与 $(\mathbb{Z}, +)$ 同构，有限 n 阶循环群与 $(\mathbb{Z}_n, +)$ 同构. 由此推得同阶 (有限或无限) 循环群必互相同构.*

以下我们以 Z 表示无限循环群，Z_n 表示有限 n 阶循环群. 关于循环群的其它基本事实是

定理 3.9 *循环群的子群仍为循环群. 无限循环群 Z 的子群除 1 以外都是无限循环群，且对每个 $s \in \mathbb{N}$，对应有一个子群 $\langle a^s \rangle$. 有限 n 阶循环群 Z_n 的子群的阶是 n 的因子，且对每个 $m \mid n$，存在唯一的 m 阶子群 $\langle a^{n/m} \rangle$.*

循环群的子群都是全不变子群.

定理 3.10 *循环群的自同构群是交换群. 无限循环群 Z 只有两个自同构，$\text{Aut}(Z) \cong Z_2$. 有限循环群 Z_n 有 $\varphi(n)$ 个自同构 (这里 φ 是 Euler φ 函数)，$\text{Aut}(Z_n)$ 同构于与 n 互素的 mod n 的同余类的乘法群.*

证 设 a 是该循环群的生成元. 则它的每个自同构由 a 的像唯一确定. 显然, 映射 $a \mapsto a^i$ 是自同构 $\Longleftrightarrow$ $\langle a^i \rangle = \langle a \rangle$. 因为 Z 只有两个生成元 a 和 a^{-1}, 而 Z_n 有 $\varphi(n)$ 个生成元, 故得结论. □

§3.3 变换群和置换群

群论的研究从变换群开始, 抽象群的概念也是从变换群的概念发展来的.

一个 (有限或无限) 集合 M 到自身上的一一映射叫做集合 M 的 *变换*.

命题 3.11 *集合 M 的全体变换依映射的乘法组成一个群 S_M.*

我们称 S_M 的任一子群为集合 M 的一个 *变换群*.

定理 3.12 (Cayley) *任一群 G 都同构于一个变换群.*

证 作 G 的右正则表示 $R: g \mapsto R(g)$, 其中 $R(g)$ 是 G 的变换: $x \mapsto xg$, $\forall x \in G$. 容易看出 R 是 G 到 S_G 内的同构映射. □

这个定理说明抽象群概念的外延从同构意义上说并不比变换群的外延来得大.

我们称有限集合的变换为 *置换*, 有限集合上的变换群为 *置换群*.

关于置换的下述初等事实是应该熟知的:

设 $M = \{1, 2, \cdots, n\}$, $i_1, i_2, \cdots, i_s \in M$, 我们以 $(i_1 i_2 \cdots i_s)$ 表示集 M 的一个 *s-轮换*, 即把 i_1 变到 i_2, i_2 变到 $i_3, \cdots$, i_s 变到 i_1, 而把 M 中其余元素保持不变的置换. 并称 2-轮换为 *对换*. 有

命题 3.13 *(1) M 的任一置换可表成互不相交的轮换的乘积, 且若不计次序, 分解式是唯一的;*

(2) M 的任一置换可表成若干个对换的乘积, 且同一置换的不同分解式中对换个数的奇偶性是确定的. 分解式中对换个数为奇数的置换叫做奇置换, 反之叫偶置换.

命题 3.14 (1) $(i_1i_2\cdots i_s)=(i_1i_2)(i_1i_3)\cdots(i_1i_s)$;

(2) 若 $\alpha\in S_n$, 则 $\alpha^{-1}(i_1i_2\cdots i_s)\alpha=(i_1^\alpha i_2^\alpha\cdots i_s^\alpha)$.

命题 3.15 S_n 的不同共轭类与 n 的不同分划之间可建立一一对应, 设 $n_1+n_2+\cdots+n_s=n$ 是 n 的一个分划, 其中 $n_1\geq n_2\geq\cdots\geq n_s$. 则所有具有形状 $(i_1\cdots i_{n_1})(i_{n_1+1}\cdots i_{n_1+n_2})\cdots(i_{n-n_s+1}\cdots i_n)$ 的轮换分解式的置换组成 S_n 的与上述分划对应的共轭类.

n 个元素的集合 $M=\{1,2,\cdots,n\}$ 的全体偶置换组成 S_n 的一个子群 A_n 并且

$$|A_n|=\frac{1}{2}|S_n|=\frac{1}{2}n!.$$

定理 3.16 若 $n\geq 5$, 则 A_n 是单群.

证 首先证明 A_n 可由所有 3-轮换生成. 设 $1\neq\alpha\in A_n$, 因 α 是偶置换, 故 α 可表成偶数个对换的乘积, 但对任意两个不同的对换的乘积我们有

$$(ab)(ac)=(abc),\quad (ab)(cd)=(acb)(cbd),$$

其中不同的字母代表不同的元素. 这就证明了 α 可表成若干个 3-轮换的乘积.

下面证明 A_n 是单群. 为此, 设 $1\neq N\trianglelefteq A_n$. 我们将说明 N 必含有一个 3-轮换, 于是由本节末习题 8, 推知所有 3-轮换属于 N, 这样 $N=A_n$.

设 $1\neq\alpha\in N$ 是 N 中变动文字个数最少的元素. 我们来证明 α 变动的文字数必为 3, 因之 α 为 3-轮换. 研究 α 的轮换分解式:

(1) α 不是二对换之积: 若否, 不妨设 $\alpha=(12)(34)$. 取 $\beta=(345)$, (因 $n\geq 5$), 则 $\beta^{-1}\alpha^{-1}\beta\alpha=(345)\in N$, 与 α 的选择相矛盾.

(2) α 不是更多个对换之积: 若否, 可设 $\alpha=(12)(34)(56)\cdots$, 取 $\beta=(123)$, 则 $\beta^{-1}\alpha^{-1}\beta\alpha=(13)(24)$. 由 (1) 知这不可能.

至此我们证得 α 的最长轮换因子的长度 ≥ 3. 把最长轮换写在前面, 又若 α 不是 3-轮换, 则 α 的轮换分解式必有下列形状:

(i) $\alpha = (123)(45\cdots)\cdots$,

(ii) $\alpha = (1234\cdots)\cdots$.

由 α 是偶置换, 对 (i), α 变动的文字个数 ≥ 6; 而对 (ii), α 变动文字数 ≥ 5.

(3) 对 (i), 取 $\beta = (234)$, 则 $\beta^{-1}\alpha^{-1}\beta\alpha = (15324)$, 变动文字数 < 6, 与 α 的选择相矛盾, 而对 (ii), 取 $\beta = (132)$, 则 $\beta^{-1}\alpha^{-1}\beta\alpha = (143)$, 也与 α 的选择相矛盾. 因此, α 是 3-轮换. □

§3.4 线性群

设 V 是域 $\mathbf{F}$ 上 n 维线性空间, 则 V 的所有可逆线性变换对乘法组成一个群, 它同构于 $\mathbf{F}$ 上全体 n 阶可逆方阵组成的乘法群. 这个群记作 $GL(n,\mathbf{F})$, 叫做域 F 上的 n 级 **全线性群**. 这也是变换群的另一个重要的例子.

令 $SL(n,\mathbf{F})$ 为所有行列式为 1 的 n 阶方阵组成的集合, 则 $SL(n,\mathbf{F})$ 是 $GL(n,\mathbf{F})$ 的子群, 叫做 $\mathbf{F}$ 上的 n 级 **特殊线性群**.

容易验证, $SL(n,\mathbf{F}) \trianglelefteq GL(n,\mathbf{F})$, 并且

$$GL(n,\mathbf{F})/SL(n,\mathbf{F}) \cong (\mathbf{F}^{\#},\cdot).$$

又, 由线性代数得知, $GL(n,\mathbf{F})$ 的中心 Z 由所有 n 阶非零纯量阵组成. 我们称

$$PGL(n,\mathbf{F}) = GL(n,\mathbf{F})/Z$$

为 $\mathbf{F}$ 上 n 级 **射影线性群**. 又

$$PSL(n,\mathbf{F}) = SL(n,\mathbf{F})/(Z \cap SL(n,\mathbf{F}))$$

为 $\mathbf{F}$ 上 n 级 **特殊射影线性群**.

假定 $\mathbf{F} = GF(q)$, 是包含 q 个元素的有限域, 则上述各群分别记作 $GL(n,q)$, $SL(n,q)$, $PGL(n,q)$, $PSL(n,q)$.

命题 3.17 (1) $|GL(n,q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$;
(2) $|SL(n,q)| = |PGL(n,q)| = |GL(n,q)|/(q-1)$;
(3) $|PSL(n,q)| = |SL(n,q)|/(n,q-1)$.

证　设 $v_1, v_2, \cdots, v_n$ 是 $\mathbf{F}$ 上 n 维线性空间 V 的一组基. V 的可逆线性变换 α 把 $v_1, \cdots, v_n$ 仍变成 V 的一组基，于是 $v_1^\alpha, v_2^\alpha, \cdots, v_n^\alpha$ 满足

$$v_1^\alpha \neq 0,\ v_2^\alpha \notin \langle v_1^\alpha \rangle, \cdots, v_n^\alpha \notin \langle v_1^\alpha, \cdots, v_{n-1}^\alpha \rangle,$$

这就推出 (1).

为证明 (2), 只须注意到 $|\mathbf{F}^\#| = |Z| = q-1$, 由 $GL(n,q)/SL(n,q) \cong (\mathbf{F}^\#, \cdot)$ 及 $PGL(n,q)$ 的定义立得结论.

而 (3) 等价于 $|Z \cap SL(n,q)| = (n, q-1)$. 由于 Z 由纯量阵组成，上式左边是满足 $a^n = 1, a \in \mathbf{F}$, 的 a 的个数，由于 $(\mathbf{F}^\#, \cdot)$ 是循环群 (有限域的乘法群是循环群.) 由本节末习题 3 即得结论. □

关于线性群的进一步知识，将在下册第 XI 章中讲述.

§3.5　其它群例

1. 二面体群

考虑平面上正 n 边形 $(n \geq 3)$ 的全体对称的集合 D_{2n}. 它包含 n 个旋转和 n 个反射 (沿 n 条不同的对称轴). 从几何上很容易看出，D_{2n} 对于变换的乘法，即变换的连续施加来说组成一个群. 叫做 *二面体群* D_{2n}, 它包含 $2n$ 个元素.

为了弄清它的构造，我们以 a 表示绕这个正 n 边形的中心沿反时针方向旋转 $\frac{2\pi}{n}$ 的变换，则 D_{2n} 中所有旋转都可以表成 a^i 的形式，$i = 0, 1, \cdots, n-1$. 它们组成 D_{2n} 的一个 n 阶正规子群 $\langle a \rangle$. 再以 b 表示沿某一预先指定的对称轴 l 所作的反射变换，于是有

$$a^n = 1, b^2 = 1, b^{-1}ab = a^{-1}. \qquad (*)$$

最后一式表示先作反射 b, 接着旋转 $\frac{2\pi}{n}$, 然后再作反射 b, 其总的效果就相当于向反方向旋转 $\frac{2\pi}{n}$. 无论从几何上还是从群论中都容易看出,

$$D_{2n} = \langle a, b\rangle = \{b^j a^i \mid j = 0, 1; i = 0, 1, \cdots, n-1\}.$$

且 D_{2n} 中乘法依照规律:

$$b^j a^i \cdot b^s a^t = b^{j+s} a^{(-1)^s i+t}.$$

事实上, 完全抛开几何的考虑, 只知道 D_{2n} 由 a, b 生成且满足关系 (*) 就可以 (从同构的意义上说) 唯一地确定这个群. 因此我们把 (*) 叫做群 D_{2n} 的定义关系. 关于定义关系较详细的讨论见 §6.

2. 四元数群

Hamilton 四元数的单位 ±1, $\pm i$, $\pm j$, $\pm k$ 在乘法下组成一个 8 阶群, 叫做*四元数群*, 记作 Q_8. Q_8 中元素的乘法满足

$$i^2 = j^2 = k^2 = -1,\ ij = k = -ji,$$

$$jk = i = -kj,\ ki = j = -ik.$$

容易验证这个群同构于 $\mathbb{C}$ 上二阶矩阵

$$\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \pm\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, \pm\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}, \pm\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$$

在矩阵乘法之下组成的群.

若令 $i = a, j = b$, 则 $Q_8 = \langle a, b\rangle$, 且满足

$$a^4 = 1, b^2 = a^2, b^{-1}ab = a^{-1}.$$

这是 Q_8 的定义关系.

显然, Q_8 是非交换群, 但它的每个子群都是正规子群, (见本节末习题 17). 具有这种性质的群叫 Hamilton 群, 可参看附录中的研究题 3.

下述定义关系给出的群 Q_{4n} 是四元数群的推广，叫做 $4n$ 阶的广义四元数群:

$$Q_{4n}=\langle a,b\rangle, a^{2n}=1, b^2=a^n, b^{-1}ab=a^{-1}, n\geq 2.$$

3. 欧氏空间的正交变换群

n 维欧氏空间 V 的全体正交变换组成群 O_n, 它也可以看作是全体 n 阶正交方阵在乘法之下组成的群:

$$O_n=\{P\in GL(n,\mathbb{R})\mid PP^t=P^tP=I\}.$$

其中 P^t 是矩阵 P 的转置.

在 O_n 中，所有行列式为 1 的正交方阵组成子群 O_n^+. 特别地， O_3^+ 就是 3 维几何空间中所有旋转组成的群.

O_3^+ 有无穷多个有限阶子群，比如每个循环群和二面体群都可看作 O_3^+ 的子群. 但除了循环群和二面体群外， O_3^+ 只有同构于 A_4, S_4 和 A_5 的有限子群，即正四面体，正六面体 (或正八面体) 以及正十二面体 (或正二十面体) 的对称群. 欲知其详，可参看张远达著《运动群》一书.

习 题

1. 证明阶互素的二循环群的直积仍为循环群.

2. 设 p 是奇素数，求证 $\mathrm{Aut}(Z_{p^n})\cong Z_{\varphi(p^n)}$, $n\geq 1$. 而对 $p=2$, $n\geq 2$, $\mathrm{Aut}(Z_{2^n})\cong Z_2\times Z_{2^{n-2}}$.

3. 设 G 是 n 阶循环群，则 G 中方程 $x^s=1$ 恰有 (s,n) 个解.

4. 证明长为偶数的轮换是奇置换，进一步说明怎样由轮换分解式来判别置换的奇偶性.

5. 证明置换的阶等于其轮换分解式中诸轮换长度的最小公倍数.

6. 证明

(1) $S_n=\langle(1\ 2),(1\ 3),\cdots,(1\ n)\rangle$;

(2) $S_n=\langle(1\ 2\ 3\cdots\ n),(1\ 2)\rangle$;

(3) $A_n=\langle(1\ 2\ 3),(1\ 2\ 4),\cdots,(1\ 2\ n)\rangle$.

7. 找出 A_4 和 S_4 的全部子群，并指出哪些是正规子群.

8. 设 $N\trianglelefteq A_n$, N 包含一个 3-轮换 $(a\ b\ c)$, 则 N 包含所有 3-轮换.

9. 设 $\alpha \in S_n$，如果 α 的轮换分解式中有 n_1 个长为 l_1 的轮换，n_2 个长为 l_2 的轮换，$\cdots$，n_s 个长为 l_s 的轮换 (包括长为 1 的轮换). 求 $|C_{S_n}(\alpha)|$ 及 α 所在的共轭类的长.

10. 设 $\alpha \in A_n$，则 α 在 S_n 中所属的共轭类整个属于 A_n. 证明这个共轭类在 A_n 中至多分裂成两个 (长度相等的) A_n 的共轭类，并且它分裂成两个共轭类的充分必要条件是 $C_{S_n}(\alpha) \subseteq A_n$，或者等价地，$C_{S_n}(\alpha)$ 不含奇置换. 再证明 $C_{S_n}(\alpha)$ 不含奇置换的充分必要条件是在 α 的轮换分解式中诸轮换的长度皆为奇数且互不相等.

11. 找出 A_5, A_6, S_5, S_6 的全部共轭元素类.

12. 通过分析 A_5, A_6 中诸共轭类的长度证明它们是单群.

13. 证明循环群 $\langle(1\ 2\ \cdots\ n)\rangle$ 在对称群 S_n 中的中心化子等于自身.

14. 设 p 是素数，$G = \langle a\rangle$ 是 p^n 阶循环群，则 G 的所有子群可排成下面的群列

$$1 < \langle a^{p^{n-1}}\rangle < \langle a^{p^{n-2}}\rangle < \cdots < \langle a\rangle = G.$$

于是 G 只有唯一的极大子群 $\langle a^p\rangle$. 反之，极大子群唯一的有限群只有素数幂阶循环群 (极大子群的定义见本章 §7 中定义 7.2).

15. 任一有限循环群都可分解为素数幂阶循环子群的直积，但素数幂阶循环群不能分解为两个真子群的直积.

16. 设 $U \le C \trianglelefteq G$, C 是循环群，则 $U \trianglelefteq G$.

17. 证明四元数群 Q_8 的每个子群都是正规子群.

18. 验证

$$G = \left\{ \begin{pmatrix} \eta^k & 0 \\ 0 & \eta^{-k} \end{pmatrix}, \begin{pmatrix} 0 & \eta^k \\ \eta^{-k} & 0 \end{pmatrix} \;\middle|\; \eta = e^{\frac{2k\pi}{n}},\ k = 0, 1, \cdots, n-1 \right\}$$

对矩阵乘法成群，并且 $G \cong D_{2n}$.

19. 证明 $D_{2^{n+1}}, n \ge 2$ 的每个非循环真正规子群的指数皆为 2.

20. 有限群 G 是二面体群的充分必要条件是 G 可由两个 2 阶元素生成.

§4. 交换群，换位子

§4.1 有限交换群的构造

在抽象代数课程中，我们从模论的观点证明了有限生成交换群可分解为循环群的直积. 现在我们再对有限群的情形给这个定理一个群论证明. 为此，先引进下述概念：

定义 4.1 设 p 是素数. 称群 G 的元素 a 为 *p-元素*, 如果 $o(a)$ 是 p 的方幂; 而称 a 为 *p'-元素*, 如果 $(o(a),p)=1$.

由此定义, 单位元素 1 既是 p-元素, 又是 p'-元素. 而且一般说来, 群中也有很多元素既非 p-元素, 也非 p'-元素.

定义 4.2 称群 G 为 *p-群*, 如果 G 的每个元素皆为 p-元素.

定义 4.3 称 p-群 S 为群 G 的 *Sylow p-子群*, 如果 S 是 G 的极大 p-子群, 即不存在 G 的 p-子群 $S_1 > S$.

定理 4.4 *有限交换群 A 是它的 Sylow p-子群 S_p 的直积*

$$A = \bigtimes_p S_p.$$

这里 p 跑遍所有使 $S_p \neq 1$ 的素数集合, 而 "$\bigtimes$" 表直积符号.

证 首先, 因为在交换群中, p-元素的乘积和逆仍为 p-元素, 故对任意素数 p, A 的 Sylow p-子群恰由 A 中所有 p-元素组成, 即

$$S_p = \{a \in A \mid a\text{是 } p\text{-元素}\}.$$

又, 使 $S_p \neq 1$ 的素数 p 只能有有限多个 (因 A 是有限群), 并且因为交换群中 p'-元素的乘积仍为 p'-元素, 故

$$S_p \cap \prod_{q\neq p} S_q = 1.$$

因此, 据定理 2.11, 为证 A 是诸 S_p 的直积只须再证 A 可由诸 S_p 生成. 现设 $a \in A$, $o(a) = n = p_1^{\alpha_1}\cdots p_s^{\alpha_s}$. 由 $(n/p_1^{\alpha_1},\cdots,n/p_s^{\alpha_s}) = 1$, 存在整数 $x_1,\cdots,x_s$ 使 $x_1\cdot n/p_1^{\alpha_1} + \cdots + x_s \cdot n/p_s^{\alpha_s} = 1$. 于是 $a = a^1 = (a^{n/p_1^{\alpha_1}})^{x_1}\cdots(a^{n/p_s^{\alpha_s}})^{x_s}$, 其中 $a^{n/p_i^{\alpha_i}}$ 是 p_i-元素, 必属于 S_{p_i}, 于是也有 $(a^{n/p_i^{\alpha_i}})^{x_i} \in S_{p_i}$. □

至此, 我们可把注意力集中于有限交换 p-群. 我们有

命题 4.5 *设 A 是有限交换 p-群，则 A 循环 $\Longleftrightarrow$ A 中只有一个 p 阶子群.*

证 $\Rightarrow$: 显然.

$\Leftarrow$: 用对 $|A|$ 的归纳法. 设 A 只有一个 p 阶子群 P. 考虑映射 $\eta: a \mapsto a^p, a \in A$, 易验证 η 是 A 的自同态，而 $\mathrm{Ker}\,\eta = P$. 由同态定理有 $A/P \cong A^\eta$, 于是 $|A : A^\eta| = p$. 若 $A^\eta = 1$, 当然 A 循环；而若 $A^\eta \neq 1$, 必有 $P \leq A^\eta$. 由归纳假设，A^η 循环. 设 $A^\eta = \langle b \rangle$, 再设 a 是在 η 之下 b 的任一原像，即 $a^\eta = a^p = b$, 于是 $|\langle a \rangle : A^\eta| = p$. 又已证 $|A : A^\eta| = p$, 故 $A = \langle a \rangle$ 是循环群. □

引理 4.6 *设 A 是有限交换 p 群，非循环，a 是 A 中最高阶元素，则存在 $B \leq A$ 使 $A = \langle a \rangle \times B$.*

证 用对 $|A|$ 的归纳法. 由 A 非循环，据命题 4.5, A 中至少含有两个 p 阶子群. 设 P 是不含于 $\langle a \rangle$ 的一个 p 阶子群. 作 $\overline{A} = A/P$, aP 仍为 $\overline{A}$ 之最高阶元素. 因为 $|\overline{A}| < |A|$, 故存在 $\overline{B} \leq \overline{A}$. 使 $\overline{A} = \langle a \rangle P/P \times \overline{B}$. 令 $\overline{B} = B/P$, 于是得 $B \geq P$, 且 $A = \langle a \rangle B$. 为完成证明只须证 $\langle a \rangle \cap B = 1$. 由 $\overline{A}$ 的上述直积分解知 $\langle a \rangle \cap B \leq P$, 故 $\langle a \rangle \cap B = P$ 或 1. 但因 $P \not\leq \langle a \rangle$, 故只能有 $\langle a \rangle \cap B = 1$. 这时有 $A = \langle a \rangle \times B$, 得证. □

定理 4.7 *有限交换 p-群 A 可以分解为循环子群的直积*

$$A = \langle a_1 \rangle \times \cdots \times \langle a_s \rangle, \qquad (*)$$

并且直因子的个数 s 以及诸直因子的阶 $p^{e_1}, \cdots, p^{e_s}$ (不妨设 $e_1 \geq \cdots \geq e_s$) 由 A 唯一决定，叫做 A 的型不变量. 而元素 $\{a_1, \cdots, a_s\}$ 叫做 A 的一组基底.

证 由引理 4.6 即得可分解性. 为证唯一性，我们用归纳法并引进 A 的两个全不变子群

$$\Omega_1(A) = \{a \in A \mid a^p = 1\}, \quad \mho_1(A) = \{a^p \mid a \in A\}.$$

实际上，它们分别为自同态 $\eta: a \mapsto a^p$ 的核和像集.

由 A 的分解式 (*) 易验证

$$\begin{aligned}\Omega_1(A) &= \langle a_1^{p^{e_1-1}}\rangle \times \cdots \times \langle a_s^{p^{e_s-1}}\rangle, \\ \mho_1(A) &= \langle a_1^p\rangle \times \cdots \times \langle a_s^p\rangle.\end{aligned}$$

由前式得 $|\Omega_1(A)| = p^s$. 因为 p^s 是由 A 唯一确定的子群 $\Omega_1(A)$ 的阶，得 s 的不变性. 再由后式及归纳假设得 $a_1^p, \cdots, a_s^p$ 的阶 $p^{e_1-1}, \cdots, p^{e_s-1}$ 是被 $\mho_1(A)$, 从而也是被 A 唯一决定的，因而 $p^{e_1}, \cdots, p^{e_s}$ 也被 A 唯一决定. □

推论 4.8 *有限交换群 A 的 Sylow p-子群的阶为 p 的方幂.*

(证略)

由定理 4.4 和定理 4.7 很容易推出一般的有限交换群的分解定理，即本节末习题 1. 那个定理经常更为有用.

§4.2 换位子和可解群

设 G 为任意群，$a, b \in G$. 我们规定

$$[a, b] = a^{-1}b^{-1}ab,$$

叫做元素 a 和 b 的换位子. 再令

$$G' = \langle [a, b] \mid a, b \in G\rangle,$$

称为 G 的换位子群或导群. 易验证

定理 4.9 *G' 是 G 的全不变子群，并且若 $N \trianglelefteq G$, 则 G/N 是交换群 $\iff N \geq G'$.*

由此，G 是交换群 $\iff G' = 1$.

我们还可归纳地定义 G 的 n 阶换位子群:

$$G^{(0)} = G, \qquad G^{(n)} = (G^{(n-1)})', \quad n \geq 1.$$

定义 4.10 称群 G 为 **可解群**, 如果存在正整数 n 使 $G^{(n)}=1$.

引理 4.11 设 $N\trianglelefteq G$, $n\geq 0$, 则 $(G/N)^{(n)}=G^{(n)}N/N$.

定理 4.12 可解群的子群和商群仍为可解群.

下面关于可解群的一些简单的事实请读者自行证明.

命题 4.13 (1) 设 $N\trianglelefteq G$, N 和 G/N 均可解, 则 G 可解;

(2) 设 $M\trianglelefteq G$, $N\trianglelefteq G$, G/M 和 G/N 均可解, 则 $G/M\cap N$ 亦可解;

(3) 设 M,N 是 G 的可解正规子群, 则 MN 亦然. 由此得出有限群 G 的所有可解正规子群的并 $\mathrm{rad}(G)$ 仍为 G 的可解正规子群, 叫做 G 的根基. 而 $G/\mathrm{rad}(G)$ 不存在非单位的可解正规子群;

(4) 可解单群必为素数阶循环群.

习 题

1. 证明任一有限交换群 G 均可表成下列形状

$$G=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_s\rangle,$$

其中 $o(a_i)\bigm| o(a_{i+1})$, $i=1,2,\cdots,s-1$. 叙述并证明关于这种分解式的唯一性定理.

2. 设 G 是有限交换群, 则 G 中存在阶为 $\exp G$ 的元素.

3. 有限交换群 G 是循环群 $\Longleftrightarrow$ $|G|=\exp G$.

4. 证明有限交换群可由其所有最高阶元素生成.

5. 设 $A=\langle a\rangle\times\langle b\rangle$, $a^{p^3}=1$, $b^p=1$. 又设 $K=\langle a^pb\rangle$. 证明不可能选到 A 的一组基和 K 的一组基, 使得 K 的基元素是 A 的某个基元素的方幂.

6. 设交换 p-群 G 的型不变量为 (p^4,p^3), 问 G 包含多少个 p^2 阶子群?

7. 设 $G=A\times B$ 则 $G'=A'\times B'$.

8. 证明域的乘法群的有限子群皆为循环群.

9. 设 G 是群, $a,b,c\in G$, 则有

(1) $[ab,c]=[a,c]^b[b,c]$;

(2) $[a,bc]=[a,c][a,b]^c$.

10. 设 G 是群， $a,b\in G$ 且 $[a,b]\in Z(G)$, 又设 n 是正整数. 则有
(1) $[a^n,b]=[a,b]^n$;
(2) $[a,b^n]=[a,b]^n$;
(3) $(ab)^n=a^nb^n[b,a]^{\binom{n}{2}}$.

§5. 自同构

§1 末尾已经讲到自同构群的概念，本节讲述关于自同构的一些简单性质，并将介绍全形和完全群的概念.

§5.1 自同构

设 G 是群， $\mathrm{Aut}(G)$ 是其自同构群， $\mathrm{Inn}(G)$ 是其内自同构群. 和 §1 一样，我们以 $\sigma(g)$ 表示由元素 g 诱导出的 G 的内自同构. 由 §2 习题 7 知

$$\mathrm{Inn}(G)\cong G/Z(G).$$

命题 5.1 设 $g\in G,\alpha\in\mathrm{Aut}(G)$, 则 $\alpha^{-1}\sigma(g)\alpha=\sigma(g^\alpha)$.

证 因 α 是 G 的自同构，故对任意的 $x\in G$, 存在 $y\in G$ 使 $y^\alpha=x$. 于是

$$\begin{aligned}x^{\alpha^{-1}\sigma(g)\alpha} &= (y^\alpha)^{\alpha^{-1}\sigma(g)\alpha}=y^{\sigma(g)\alpha}=(g^{-1}yg)^\alpha\\ &= (g^\alpha)^{-1}y^\alpha g^\alpha=(g^\alpha)^{-1}xg^\alpha=x^{\sigma(g^\alpha)},\end{aligned}$$

所以 $\alpha^{-1}\sigma(g)\alpha=\sigma(g^\alpha)$. □

由命题 5.1 立得

定理 5.2 $\mathrm{Inn}(G)\trianglelefteq\mathrm{Aut}(G)$.

定义 5.3 我们称 $\mathrm{Aut}(G)\setminus\mathrm{Inn}(G)$ 中的元素为 G 的外自同构，而称 $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ 为 G 的外自同构群.

有下述著名的

Schreier 猜想：设 G 是有限单群，则 G 的外自同构群为可解群.

由定理 3.10, 这个猜想对于有限交换单群，即素数阶循环群来说当然是成立的. 并且人们已经对所有已知的非交换单群进行了验证. 现在单群分类问题已经解决，于是这个猜想已经成为定理. 当然，不用逐一检验的方法，寻找它的一般性的证明目前仍是一件吸引人的工作.

关于自同构的下述结果是经常要用到的.

定理 5.4 设 $N \trianglelefteq G, \alpha \in \mathrm{Aut}(G)$. 如果 $N^\alpha = N$, 则映射 $\bar{\alpha}: Ng \mapsto Ng^\alpha$ 是 G/N 的自同构，叫做由 α 诱导出的 G/N 的自同构.

(证明系直接验证，从略.)

定理 5.5 设 $N \trianglelefteq G, \alpha \in \mathrm{Aut}(G)$. 如果 $\alpha|_N = 1$, 且由 α 诱导的 G/N 的自同构 $\bar{\alpha} = 1$, 则 $\tau(g) = g^{-1}g^\alpha \in Z(N)$, $\forall g \in G$, 并且 τ 可看成 G/N 的函数，即在 N 的每个陪集上，τ 的取值都相同.

证 设 $g \in G, n \in N$. 因 $N \trianglelefteq G$, 故 $gng^{-1} \in N$. 这样

$$gng^{-1} = (gng^{-1})^\alpha = g^\alpha n^\alpha (g^{-1})^\alpha = g^\alpha n (g^{-1})^\alpha.$$

于是 $g^{-1}g^\alpha n = ng^{-1}g^\alpha$. 又由 $g^\alpha N = gN$ 得 $g^{-1}g^\alpha \in N$, 故 $g^{-1}g^\alpha \in Z(N)$. 因为对任意的 $g \in G, n \in N$ 有

$$\tau(gn) = (gn)^{-1}(gn)^\alpha = n^{-1}g^{-1}g^\alpha n = g^{-1}g^\alpha = \tau(g).$$

故在 N 的每个陪集上，τ 的取值都相同. □

推论 5.6 设 G, N, α 同定理 5.5, 如果又有

$$(o(\alpha), |Z(N)|) = 1,$$

则 $\alpha = 1$.

证 设 $\exp Z(N) = m$, 则对任意的 $g \in G$, 有

$$g^{\alpha^m} = g\tau(g)^m = g,$$

故 $\alpha^m = 1$. 因为 $\exp Z(N) \mid |Z(N)|$, 故 $\alpha^{|Z(N)|} = 1$. 于是 $o(\alpha) \mid |Z(N)|$. 但由 $(o(\alpha), |Z(N)|) = 1$, 只能有 $o(\alpha) = 1$, 即 $\alpha = 1$ □

这个推论经常用来研究 p-群的 p'-自同构，即其阶与 p 互素的自同构.

定理 5.7 设 $H \leq G$, 则 $N_G(H)/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的一个子群.

证 设 $g \in N_G(H)$, 则 $\sigma(g): h \mapsto h^g$ 是 H 的自同构. 并且显然 $g \mapsto \sigma(g)$ 是 $N_G(H)$ 到 $\mathrm{Aut}(H)$ 内的同态，其核为

$$\begin{aligned}\mathrm{Ker}\,\sigma &= \{g \in N_G(H) \mid h^g = h, \forall h \in H\} \\ &= C_{N_G(H)}(H) = C_G(H) \cap N_G(H).\end{aligned}$$

但明显的有 $C_G(H) \leq N_G(H)$, 故 $\mathrm{Ker}\,\sigma = C_G(H)$. 于是由同态基本定理

$$N_G(H)/C_G(H) \cong \sigma(N_G(H)) \leq \mathrm{Aut}(H).$$

□

这个定理虽然简单，但十分有用. 在下一章中将会遇到它的若干应用. 为了简便，人们常称这个定理为“N/C 定理”.

§5.2 全形

我们知道，群 G 的自同构不一定都是内自同构. 因此提出下列问题：是否存在一个群 $G^* \geq G$, 且 $G \trianglelefteq G^*$, 使得 G 的每个自同构都可由 G^* 的内自同构限制在 G 上得到？这个问题的答案是肯定的. 所谓群的全形就是一个满足上述条件的扩群，下面我们不加证明地给出全形的理论要点，请读者自己把证明补足.

考虑 G 上全体一一变换组成的群 S_G. 以 $R: G \to S_G$ 表示 G 的右正则表示，即 $x^{R(g)} = xg$, $\forall x, g \in g$. 以 $L: G \to S_G$ 表 G 的左正则表示，即 $x^{L(g)} = gx$, $\forall x, g \in G$. 则这两个映射的像集 $R(G)$ 和 $L(G)$ 都是 S_G 的子群. 由 Cayley 定理，$G \cong R(G)$; 又易验证 $L(G)$ 与 G 反同构，即 L 是 G 到 $L(G)$ 上的一一映射，满足 $L(gh) = L(h)L(g)$, $\forall g, h \in G$.

定义 5.8 称 $\mathrm{Hol}(G) = N_{S_G}(R(G))$ 为 G 的 全形.

定理 5.9 (1) $R(G) = C_{S_G}(L(G))$, $L(G) = C_{S_G}(R(G))$, 从而

$$L(G) \le \mathrm{Hol}(G);$$

(2) $\mathrm{Hol}(G)$ 中保持 1 不变的元素组成的子群是 $\mathrm{Aut}(G)$, 于是

$$\mathrm{Hol}(G) = R(G)\mathrm{Aut}(G) \quad 且 \quad R(G) \cap \mathrm{Aut}(G) = 1.$$

如果我们把 G 和 $R(G)$ 等同看待，那么 $\mathrm{Hol}(G)$ 就可作为上述问题中要找的群 G^*.

§5.3 完全群

定义 5.10 称群 G 为 完全群, 如果 $Z(G) = 1$, 且 $\mathrm{Aut}(G) = \mathrm{Inn}(G)$.

例 5.11 对称群 S_3 是完全群.

证 因为 $S_3 = \langle a, b\rangle$, 有定义关系

$$a^3 = 1, b^2 = 1, b^{-1}ab = a^{-1},$$

故若 $\alpha \in \mathrm{Aut}(S_3)$, 则 a^α, b^α 必满足同一定义关系. 由 a, b 的阶推知，a^α 只能为 $a^{\pm 1}$, b^α 只可能为 b 或 $ba^{\pm 1}$. 又因为 α 可由 a^α, b^α 唯一确定，于是 α 至多有六种选取方法. 这说明 $|\mathrm{Aut}(S_3)| \le 6$. 但因 $Z(S_3) = 1$, $\mathrm{Inn}(S_3) \cong S_3$, 于是 $|\mathrm{Inn}(S_3)| = |S_3| = 6$, 故只能有 $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3)$. □

事实上，我们能够证明，对称群 S_n, 只要 $n \neq 6$ 都是完全群.

定理 5.12 设 G 是非交换单群，则 $\mathrm{Aut}(G)$ 是完全群.

证 因 G 是非交换单群，有 $Z(G)=1$，由此 G 的内自同构映射 σ 是 G 到 $\mathrm{Inn}(G)$ 的同构. 记 $I=\mathrm{Inn}(G)$，$A=\mathrm{Aut}(G)$. 有 $I\trianglelefteq A$. 我们分下面几步证明定理.

(1) $C_A(I)=1$.

设 $\zeta\in C_A(I)$，则 $\zeta^{-1}\sigma(g)\zeta=\sigma(g)$，$\forall g\in G$. 由命题 5.1 得 $\sigma(g^{\zeta})=\sigma(g)$，$\forall g\in G$，注意到 σ 是 G 到 I 上的同构，就得到 $g^{\zeta}=g$，$\forall g\in G$，于是 $\zeta=1$.

(2) 设 $a\in\mathrm{Aut}(A)$，则 $I^a=I$.

如果 $I^a\neq I$，由 $I^a\trianglelefteq A^a=A$，故 $I\neq I^a\cap I\trianglelefteq I$. 由 I 是单群知 $I^a\cap I=1$. 这时据定理 2.11，A 的子群 $\langle I^a,I\rangle=I^a\times I$，于是 $I^a\leq C_A(I)=1$，矛盾.

(3) 设 $a\in\mathrm{Aut}(A)$，证明 $a\in\mathrm{Inn}(A)$.

由 (2)，$a|_I\in\mathrm{Aut}(I)$. 对于任意的 $\sigma(g)\in I$，令 $\sigma(g)^a=\sigma(g^{\alpha})$，这样确定了 G 到自身的映射 α. 易验证 α 是一一映射 (略). 又由

$$\begin{aligned}\sigma((gh)^{\alpha}) &= \sigma(gh)^a=(\sigma(g)\sigma(h))^a=\sigma(g)^a\sigma(h)^a\\ &= \sigma(g^{\alpha})\sigma(h^{\alpha})=\sigma(g^{\alpha}h^{\alpha}),\end{aligned}$$

知 α 是 G 的自同构，故 $\alpha\in A$. 以 $\Sigma(\alpha)$ 记由 α 诱导出的 A 的内自同构. 再令 $b=a\Sigma(\alpha)^{-1}\in\mathrm{Aut}(A)$，我们来证明 $b=1$，从而 $a=\Sigma(\alpha)\in\mathrm{Inn}(A)$. 这只要证对任意的 $\eta\in A$，有 $\eta^{a\Sigma(\alpha)^{-1}}=\eta$，或者对任意的 $g\in G$，$\eta\in A$，有 $g^{\eta^{a\Sigma(\alpha)^{-1}}}=g^{\eta}$. 而这又等价于 $\sigma(g^{\eta^{a\Sigma(\alpha)^{-1}}})=\sigma(g^{\eta})$. 因为据命题 5.1

$$\begin{aligned}\sigma(g^{\eta^{a\Sigma(\alpha)^{-1}}}) &= (\eta^{a\Sigma(\alpha)^{-1}})^{-1}\sigma(g)(\eta^{a\Sigma(\alpha)^{-1}})\\ &= (\alpha\eta^a\alpha^{-1})^{-1}\sigma(g)(\alpha\eta^a\alpha^{-1})\\ &= \alpha(\eta^a)^{-1}(\alpha^{-1}\sigma(g)\alpha)\eta^a\alpha^{-1}\\ &= \alpha(\eta^{-1})^a\sigma(g^{\alpha})\eta^a\alpha^{-1}\\ &= \alpha(\eta^{-1})^a\sigma(g)^a\eta^a\alpha^{-1}\\ &= \alpha(\eta^{-1}\sigma(g)\eta)^a\alpha^{-1}\end{aligned}$$

$$\begin{aligned} &= \alpha\sigma(g^{\eta})^{\alpha}\alpha^{-1} \\ &= \alpha\sigma(g^{\eta\alpha})\alpha^{-1} \\ &= \sigma(g^{\eta\alpha\alpha^{-1}}) \\ &= \sigma(g^{\eta}), \end{aligned}$$

定理得证. □

定理 5.12 给出一大批完全群的例子，这些群显然都不是可解群. 由例 5.11 知存在着可解完全群，而且事实上存在无穷多个这样的群. 对于可解完全群进行完全分类的工作至今尚未完成.

另外，还有一个问题：是否存在奇数阶完全群？这个为 G.A. Miller 提出的较古老的问题已被 R.S. Dark 解决，他构造了一个 $3 \cdot 9 \cdot 7^{12}$ 阶完全群 (参看 Dark 的文章 "A complete group of odd order", *Math. Proc. Camb. Phil. Soc.*, **77**(1975), 21–28.)

关于完全群的新近的发展可参看下列文章：

D.J.S. Robinson, Recent results on finite complete groups, in "Algebra, Carbondale 1980", Lecture Notes in Math. No. 848, 178–185.

习 题

1. 证明 $\mathrm{Aut}(D_8) \cong D_8$, 但 D_8 不是完全群.
2. 证明 S_4 是完全群.
3. 举例说明不同构的群可能有同构的自同构群.
4. 找一有限群 G, 它有正规子群 H, 满足 $|\mathrm{Aut}(H)| > |\mathrm{Aut}(G)|$.
5. 设 Q_8 是四元数群，证明 $\mathrm{Aut}(Q_8) \cong S_4$.
6. 设 $N \trianglelefteq G$, 并且 N 是完全群，则 N 一定是 G 的直积因子，即有 $M \leq G$, 使 $G = N \times M$.
7. 群 G 是交换群的充分必要条件是映射 $\alpha : g \mapsto g^{-1}$, $\forall g \in G$, 是 G 的自同构.
8. 设 G 是奇阶交换群， $\alpha \in \mathrm{Aut}(G)$, $\alpha^2 = 1$, 令

$$G_1 = \{g \in G \mid g^{\alpha} = g\}, \ G_2 = \{g \in G \mid g^{\alpha} = g^{-1}\},$$

则 G_1, G_2 都是 G 的子群，并且 $G = G_1 \times G_2$.

9. 在第 8 题中去掉 G 交换的条件，则仍有 $G=G_1G_2$, $G_1\cap G_2=1$, 并且 G 的每一元素 g 可唯一地表写成 G_1 的一个元素 g_1 和 G_2 的一个元素 g_2 之乘积.

10. 设 $H\leq G$, $\alpha\in \mathrm{Aut}(G)$, 满足 $(Hg)^\alpha=Hg$, $\forall g\in G$, 则

$$g^\alpha g^{-1}\in \bigcap_{x\in G} H^x,\ \forall g\in G.$$

11. 设 $\alpha\in \mathrm{Aut}(G)$, 满足 $g^{-1}g^\alpha\in Z(G)$, $\forall g\in G$, 则称 α 为 G 的中心自同构. 证明 G 的全体中心内自同构组成 $\mathrm{Aut}(G)$ 的子群，并且和 $Z(G/Z(G))$ 同构.

12. 设 α 是有限群 G 的自同构，满足

$$g^\alpha\neq g,\quad \forall g\in G\setminus\{1\}.$$

则称 α 为 G 的一个无不动点自同构. 证明这时必有 $G=\{x^{-1}x^\alpha \mid x\in G\}$.

13. 具有 2 阶无不动点自同构的有限群必为奇阶交换群.

14. 设 N 是群 G 的循环正规子群，则 N 的任一元素与 G' 的任一元素可交换.

§6. 自由群，生成元和关系

§6.1 自由群

给定集合 $X=\{x_1,\cdots,x_r\}$, 它的势 r 不一定有限或可数. 令 $X^{-1}=\{x_1^{-1},\cdots,x_r^{-1}\}$ 为另一集合，并假定 $X\cap X^{-1}=\varnothing$. 再令 $S=X\cup X^{-1}$. 我们称有限序列 $w=a_1a_2\cdots a_n$ 为 X上的字, 如果每个 $a_i\in S$. 并且规定空集也为字，叫做 空字. 规定两个字的乘积为它们的连写，易验证所有 X 上的字的集合 W 对所规定的乘法成一有单位元半群，空字是其单位元素.

称两个字 w_1 和 w_2 (以及 w_2 和 w_1) 为 邻接的, 如果它们有形状： $w_1=uv$, 而 $w_2=ux_ix_i^{-1}v$ 或 $ux_i^{-1}x_iv$, 其中 u,v 是 X 上的两个字，而 $x_i\in X$. 又规定两个字 w_1 和 w_2等价, 记作 $w_1\sim w_2$, 如果可找到有限多个字 $w_1=f_1$, $f_2,\cdots,f_{n-1}$, $f_n=w_2$, 使对 $i=1,2,\cdots,n-1$, f_i 和 f_{i+1} 是邻接的. 易验证 “$\sim$” 是等价关系，并且若 $w_1\sim w_1'$, $w_2\sim w_2'$, 则 $w_1w_2\sim w_1'w_2'$. 我们以 $[w]$ 记

字 w 所在的等价类，令 F 为所有等价类组成的集合，规定等价类的乘法为

$$[w_1][w_2] = [w_1 w_2], \tag{*}$$

就使 F 对此乘法成为一个群，叫做 X 上的 *自由群*. 请读者自行验证 F 确满足群的公理.

自由群 F 由集合 X (叫做 *自由生成系*) 的势唯一确定. 即由两个等势的集合 X_1, X_2 作为自由生成系所得到的自由群是同构的. 这个势叫做自由群 F 的 *秩*. 以后秩为 r 的自由群记作 F_r.

定理 6.1 *任一可由 r 个元素生成的群都同构于 F_r 的商群.*

证 设 $G = \langle a_1, \cdots, a_r \rangle$, 又设 r 秩自由群 F_r 的自由生成系为 $\{x_1, \cdots, x_r\}$. 规定映射 $\eta : [x_i] \mapsto a_i$, $i = 1, 2, \cdots, r$, 并把它扩展到 F_r 上. 易验证 η 是一同态映射，于是

$$G \cong F_r/\mathrm{Ker}\ \eta. \qquad \square$$

由这个定理可以看出 r 秩自由群在 r 元生成群中的地位.

下面我们不加证明地叙述自由群的一个重要定理，其证明可见 M. Hall 的《群论》 §7.2.

定理 6.2 (Schreier) *自由群的子群仍为自由群. 假定 F_r 为有限秩 r 的自由群, N 是 F_r 的有限指数子群, $|F_r : N| = n$, 则 $N \cong F_{1+n(r-1)}$.*

结合定理 6.1 和定理 6.2 可得下面的

推论 6.3 *设群 G 可由 r 个元素生成, $N \leq G$, 且 $|G : N| = n$, 则 N 可由 $1 + n(r-1)$ 个元素生成.*

§6.2 生成系及定义关系

应用自由群的概念可对群的生成系和定义关系给出更清楚的解释.

设 $G=\langle a_1,\cdots,a_r\rangle$. 作自由群 $F_r=\langle x_1,\cdots,x_r\rangle$. 由定理 6.1, $G\cong F_r/K$, 其中 K 是 F_r 的某个正规子群. 设

$$f(x_1,\cdots,x_r)=x_{i_1}^{n_1}\cdots x_{i_s}^{n_s}\in K,\ i_1,\cdots,i_s\in\{1,\cdots,r\},$$

则在 G 中成立

$$f(a_1,\cdots,a_r)=a_{i_1}^{n_1}\cdots a_{i_s}^{n_s}=1,$$

我们称等式 $f(a_1,\cdots,a_r)=1$ 为 G 中的一个**关系** (有时也称自由群 F_r 中的元素 $f(x_1\cdots,x_r)$ 为 G 的一个关系).

我们又称由自由群 G 的关系组成的一个集合 $\{f_i(a_1,\cdots,a_r)=1\mid i\in I\}$ 为 G 的一个**定义关系组**, (或称 $V=\{f_i(x_1,\cdots,x_r)\mid i\in I\}$ 为 G 的定义关系组), 如果 V 在 F_r 中的正规闭包 $V^{F_r}=K$.

上述定义说明, 由所给的生成系间的任何一组关系 V 都可唯一确定一个群, 以这组关系为定义关系组. 这个群同构于 F_r/V^{F_r}. 因此, 不存在所给的关系组互不相容的情形, 这是在很多初学群论的人中间经常发生的一种误解. 但是, 具体由给定的生成系和定义关系组来决定群, 哪怕只是决定群的阶, 一般都是十分困难的. 下面我们举几个简单的例子.

例 6.4 设 $G=\langle a\rangle$, 定义关系组为 $a^4=1$, $a^6=1$, 求 $|G|=?$

解 表面上看, 关系 $a^4=1$ 和 $a^6=1$ 是不相容的. 但由上述定义关系组的含意, 我们所求的群 G 应为秩为 1 的自由群即无限循环群 $F=\langle x\rangle$ 对于子群 $\langle x^4,x^6\rangle^F$ 的商群. 容易看出, $\langle x^4,x^6\rangle=\langle x^2\rangle$, 而因 F 交换, $\langle x^2\rangle$ 的正规闭包 $\langle x^2\rangle^F=\langle x^2\rangle$, 故

$$G\cong F/\langle x^2\rangle\cong Z_2.$$

于是 $|G|=2$. □

例 6.5 设 $G=\langle a,b\rangle$, 定义关系组为 $a^2=b^2=(ab)^n=1$, 则 $G\cong D_{2n}$.

解 因为 $G=\langle a,b\rangle=\langle ab,b\rangle$, 而

$$b^{-1}(ab)b=b^{-1}a^{-1}=(ab)^{-1}\in\langle ab\rangle,$$

所以 $\langle ab\rangle\trianglelefteq G$. 于是 $G=\langle ab,b\rangle=\langle ab\rangle\cdot\langle b\rangle$, G 中每个元素都可表成 $(ab)^ib^j$ 的形状，其中 $i=0,1,\cdots,n-1$; $j=0,1$. 由此得出 $|G|\le 2n$. 另一方面，$2n$ 阶二面体群 $D_{2n}=\langle x,y\mid x^n=y^2=1,y^{-1}xy=x^{-1}\rangle$ 对于另一组生成系 xy^{-1},y 有关系 $(xy^{-1})^2=y^2=(xy^{-1}\cdot y)^n=1$, 于是 D_{2n} 应为 G 的同态像. 但已有 $|G|\le|D_{2n}|$, 故只能有 $|G|=2n$ 且 $G\cong D_{2n}$. □

例 6.6 设 $G=\langle a,b\rangle$, 定义关系组为 $a^3=b^2=(ab)^3=1$, 则 $G\cong A_4$.

解 由 $a^3=1$ 和 $b^2=1$, G 中元素均可表成 a^i, 或 $a^iba^{\pm1}b\cdots ba^j$ 之形状，其中 $i,j=0,\pm1$. 又由 $(ab)^3=1$ 得 $ababab=1$, 由此推出 $bab=(aba)^{-1}=a^{-1}ba^{-1}$, 和 $aba=(bab)^{-1}=ba^{-1}b$. 二式可统一写成 $ba^{\pm1}b=a^{\mp1}ba^{\mp1}$. 应用这个关系式可将 $a^iba^{\pm1}b\cdots ba^j$ 化成只含一个 b 的形状，即化成 a^iba^j 的形状，于是

$$G=\{a^i,a^iba^j\mid i,j=0,\pm1\}.$$

这样，$|G|\le 3+3\times3=12$. 另一方面，在交错群 A_4 中，令 $x=(123)$, $y=(12)(34)$, 则 $xy=(243)$, 因此有关系 $x^3=y^2=(xy)^3=1$. 又显然有 $A_4=\langle x,y\rangle$, 于是 A_4 应为 G 之同态像. 但因 $|A_4|=12$, $|G|\le12$, 这就迫使 $|G|=12$ 且 $G\cong A_4$. □

例 6.7 设 $G=\langle x,y\rangle$, 定义关系组为 $xy^2=y^3x,yx^3=x^2y$, 求 $|G|=?$

解 由关系 $xy^2=y^3x$ 得

$$xy^2x^{-1}=y^3. \tag{6.1}$$

由关系 $yx^3=x^2y$ 得

$$y^{-1}x^2y=x^3. \tag{6.2}$$

据 (6.1)

$$x^2y^4x^{-2} = x(xy^2x^{-1})^2x^{-1} = xy^6x^{-1} = (xy^2x^{-1})^3 = y^9. \qquad (6.3)$$

于是 $y^{-1}x^2y^4x^{-2}y = y^{-1}y^9y = y^9$, 即

$$y^{-1}x^2y \cdot y^4 \cdot y^{-1}x^{-2}y = y^9.$$

再据 (6.2) 式，上式变为

$$x^3y^4x^{-3} = x^9.$$

再由 (6.3) 式，得

$$x^2y^4x^{-2} = x^3y^4x^{-3}.$$

于是 $xy^4x^{-1} = y^4$. 但由 (6.1), $xy^4x^{-1} = (xy^2x^{-1})^2 = y^6$, 这就推出 $y^4 = y^6$, $y^2 = 1$. 再用 (6.1) 式，又得 $y^3 = xy^2x^{-1} = 1$, 于是得到 $y = 1$. 代入 (6.2) 式，即得 $x^3 = x^2$, 于是 $x = 1$. 这样 $G = \langle x, y\rangle = 1$, $|G| = 1$. □

习　题

1. 设 $G = \langle a, b\rangle$, 定义关系组为 $a^3 = b^3 = (ab)^2 = 1$. 证明 $G \cong A_4$.
2. 设 $G = \langle a, b\rangle$, 定义关系组为 $a^4 = b^2 = (ab)^3 = 1$. 证明 $G \cong S_4$.
3. 设 $G = \langle a, b\rangle$, 定义关系组为 $a^5 = b^2 = (ab)^3 = 1$. 证明 $G \cong A_5$.
4. 设 $G = \langle a_1, a_2 \cdots, a_{n-1}\rangle$, 定义关系组为 $a_i^2 = 1$, $(a_ia_{i+1})^3 = 1$, $(a_ia_j)^2 = 1$, 其中 $i, j = 1, 2, \cdots, n-1$; 但 $j - i > 1$. 则 $G \cong S_n$.
5. 证明有限生成群的有限指数子群仍为有限生成群.

§7. 例题选讲

为了使读者逐步熟悉有限群中所使用的方法和技巧，我们在本节中有选择地讲一些例题.

例 7.1 设 G 是有限群，$H < G$, 则 H 的所有共轭子集的并为 G 的真子集.

证 设 $H_1 = H, H_2, \cdots, H_k$ 是与 H 共轭的全部子群. 由定理 1.24, $k = |G : N_G(H)|$. 因为 $N_G(H) \geq H$ 有

$$k = |G : N_G(H)| \leq |G : H|.$$

于是

$$\begin{aligned} \left|\bigcup_{i=1}^{k} H_i\right| &= 1 + \left|\bigcup_{i=1}^{k}(H_i - \{1\})\right| \\ &\leq 1 + k(|H| - 1) \\ &\leq 1 + |G : H|(|H| - 1) \\ &= |G| - |G : H| + 1. \end{aligned}$$

因为 $H < G$, 故 $|G : H| > 1$. 于是有

$$\left|\bigcup_{i=1}^{k} H_i\right| < |G|,$$

即 $\bigcup_{i=1}^{k} H_i$ 是 G 的真子集. □

定义 7.2 称群 G 的子群 H 为 G 的 **极大子群**, 如果 $H < G$, 并且由 $H \leq K \leq G$ 可推出 $H = K$ 或 $K = G$.

例 7.3 设 G 是有限群, 它的任二极大子群都在 G 中共轭, 则 G 为循环群.

证 任取 G 的极大子群 H, 由例 7.1,

$$\bigcup_{x \in G} H^x \subsetneq G.$$

取 $a \in G - \bigcup_{x \in G} H^x$, 则必有 $G = \langle a \rangle$, 即 G 是循环群. 因若不然, 有 $\langle a \rangle < G$, 则存在 G 的极大子群 $M \geq \langle a \rangle$. 但由假设, M 与 H 共轭, 即对某个 $y \in G$ 有 $M = H^y$. 于是 $a \in \bigcup_{x \in G} H^x$, 与 a 的选择矛盾. □

例 7.4 设 G 是群, $M \trianglelefteq G, N \trianglelefteq G$, 且 $M \cap N = 1$. 则对任意的 $m \in M, n \in N$, 有 $mn = nm$.

证 考虑元素

$$m^{-1}n^{-1}mn = (m^{-1}n^{-1}m)n = m^{-1}(n^{-1}mn).$$

由 $N \trianglelefteq G$, 有 $m^{-1}n^{-1}m \in N$; 而由 $M \trianglelefteq G$, 有 $n^{-1}mn \in M$. 于是 $(m^{-1}n^{-1}m)n \in N$, $m^{-1}(n^{-1}mn) \in M$, 即 $m^{-1}n^{-1}mn \in M \cap N$. 又由 $M \cap N = 1$ 得 $m^{-1}n^{-1}mn = 1$, 即 $mn = nm$. □

例 7.5 设 $M \trianglelefteq G$, $N \trianglelefteq G$, 则

$$G/(M \cap N) \lesssim (G/M) \times (G/N).$$

(符号 "$H \lesssim G$" 表 "H 同构于 G 的子群.")

证 考虑群 G 到 $(G/M) \times (G/N)$ 内的映射 σ:

$$g^{\sigma} = (gM, gN),\ \forall g \in G.$$

易验证 σ 是 G 到 $(G/M) \times (G/N)$ 内的同态, 其同态核 $\operatorname{Ker} \sigma = M \cap N$. 于是由同态基本定理得

$$G/(M \cap N) \lesssim (G/M) \times (G/N).$$

□

定义 7.6 设 p 是素数, Z_p 是 p 阶循环群. 又设 n 是正整数,

$$G = \underbrace{Z_p \times Z_p \times \cdots \times Z_p}_{n个}.$$

则显然 G 是 p^n 阶交换群, 称为 p^n 阶初等交换 p-群. 换言之, 我们称型不变量为 $(p, p, \cdots, p)$ 的交换 p-群为初等交换 p 群.

容易验证, 有限交换群 G 是初等交换 p-群的充分必要条件为 $\exp G = p$.

例 7.7 设 G 是 p^n 阶初等交换 p-群，则

(1) G 同构于 $GF(p)$ 上 n 维向量空间的加法群；

(2) G 的 p^m 阶 $(1 \le m \le n)$ 子群的个数

$$\begin{bmatrix} n \\ m \end{bmatrix}_p = \frac{(p^n-1)(p^{n-1}-1)\cdots(p^{n-m+1}-1)}{(p^m-1)(p^{m-1}-1)\cdots(p-1)}.$$

证 (1) 设 $Z_p = \langle a \rangle$ 是 p 阶循环群，则

$$G = \underbrace{Z_p \times \cdots \times Z_p}_{n\text{个}} = \{(a^{x_1}, \cdots, a^{x_n}) \mid x_i \in \mathbb{Z}_p\}.$$

又设

$$V = \{(x_1, \cdots, x_n) \mid x_i \in GF(p) = \mathbb{Z}_p\}$$

是 $GF(p)$ 上 n 维向量空间. 易验证映射

$$\sigma : (x_1, \cdots, x_n) \mapsto (a^{x_1}, \cdots, a^{x_n})$$

是 $(V,+)$ 到 G 上的同构，于是 $G \cong (V,+)$.

(2) 在 (1) 中的同构 σ 之下，G 的 p^m 阶子群与 V 的 m 维子空间之间有一个一一对应. 于是 G 的 p^m 阶子群的个数等于 V 的 m 维子空间的个数. 因为 V 中任意 m 个线性无关的向量生成一个 m 维子空间，故 V 中 m 维子空间的个数等于在 V 中选取 m 个 (有序的) 线性无关向量的不同选取方法的个数除以 m 维空间中不同 (有序的) 基的选取方法的个数. 因此得到

$$\begin{aligned}\begin{bmatrix} n \\ m \end{bmatrix}_p &= \frac{(p^n-1)(p^n-p)\cdots(p^n-p^{m-1})}{(p^m-1)(p^m-p)\cdots(p^m-p^{m-1})} \\ &= \frac{(p^n-1)(p^{n-1}-1)\cdots(p^{n-m+1}-1)}{(p^m-1)(p^{m-1}-1)\cdots(p-1)}\end{aligned}$$

□

例 7.8 初等交换 p-群 G 是特征单群.

证 根据例 7.7(1)，若 $|G| = p^n$，则 G 同构于 $GF(p)$ 上的 n 维向量空间的加法群. 这时，G 的自同构相当于 V 的满秩线性

变换，而 G 的特征子群则对应于 V 的这样的子空间，它在 V 的所有满秩线性变换之下都映到自身. 显然，这样的子空间只能是平凡子空间，于是，G 的特征子群也只能是平凡子群，即 G 是特征单群. □

例 7.9 设 $G = N_1 \times N_2 \times \cdots \times N_s$, 其中 $N_1, N_2, \cdots, N_s$ 是彼此同构的非交换单群，则

(1) G 的任一非单位正规子群 K 均有形状

$$N_{i_1} \times N_{i_2} \times \cdots \times N_{i_t}, 1 \le i_1 < i_2 < \cdots < i_t \le s;$$

(2) G 是特征单群.

证 (1) 设 $g = g_1g_2\cdots g_s \in K$, 其中 $g_1 \in N_1, g_2 \in N_2, \cdots, g_s \in N_s$, 并且对某个 j 有 $g_j \ne 1$. 则 g 在 G 中的正规闭包 g^G 必包含 N_j 中的某一非单位元素. 这是因为对任意的 $x \in N_j$, g^G 包含元素

$$g^{-1}g^x = (g_1g_2\cdots g_s)^{-1}(g_1g_2\cdots g_s)^x = g_j^{-1}g_j^x = [g_j, x].$$

因为 N_j 是非交换单群，$Z(N_j) = 1$, 故至少存在一个 $x \in N_j$ 使 $h_j = [g_j, x] \ne 1$. 再由 N_j 是单群，有 $h_j^{N_j} = N_j$. 于是 $K \ge g^G \ge N_j$. 概括起来说，即如果 K 中有一元素 g, 使得它在直积分解中的第 j 个分量 $g_j \ne 1$, 则必有 $K \ge N_j$. 这就立即推出 K 必有形状 $N_{i_1} \times \cdots \times N_{i_t}$, 其中 N_{i_j} 在分解式中出现的充要条件是 K 中有一元素，它的第 i_j 个分量 $\ne 1$.

(2) 用反证法. 设 G 有一非平凡特征子群 K, 则 K 首先是 G 的正规子群，于是由 (1), K 是若干个直因子的乘积. 为简便计，不妨设

$$K = N_1 \times \cdots \times N_{t-1},\ 1 < t \le s.$$

由题设，假定 α 是 N_1 到 N_t 上的同构，则容易验证下述映射 β 是 G 的自同构：若 $g = g_1g_2\cdots g_s$, 其中 $g_1 \in N_1, g_2 \in N_2, \cdots, g_s \in N_s$, 则规定

$$g^\beta = (g_1g_2\cdots g_s)^\beta = g_1^\alpha g_2 \cdots g_{t-1} g_t^{\alpha^{-1}} g_{t+1} \cdots g_s.$$

但因 $K^{\beta} = N_t N_2 \cdots N_{t-1} \neq K$, 故 K 不是特征子群. 矛盾. □

例 7.10 每个真子群皆交换的有限非交换群必含有非平凡正规子群.

证 用反证法. 设结论不真, 则 G 必为非交换单群. 我们来分析 G 的极大子群的性质. 以下用符号 $M \lessdot G$ 表示 M 是 G 的极大子群.

(1) 若 $M \lessdot G$, 则 $N_G(M) = M$. 于是与 M 共轭的子群个数为 $|G:M|$: 因为 $M \lessdot G$, G 非交换, 必有 $M \neq 1$. 于是 $N_G(M) < G$. 又因 $N_G(M) \geq M$, 由 M 的极大性即得 $N_G(M) = M$.

(2) 若 $M_1 \lessdot G$, $M_2 \lessdot G$, $M_1 \neq M_2$, 则 $M_1 \cap M_2 = 1$: 由定理条件, M_1, M_2 皆为交换群. 因为交换群的子群皆正规, 有 $M_1 \cap M_2 \trianglelefteq M_1$, $M_1 \cap M_2 \trianglelefteq M_2$. 由此得 $M_1 \cap M_2 \trianglelefteq \langle M_1, M_2 \rangle$. 而因 M_1, M_2 是不同的极大子群, 当然有 $\langle M_1, M_2 \rangle = G$, 于是 $M_1 \cap M_2 \trianglelefteq G$. 最后由 G 是单群, 即得 $M_1 \cap M_2 = 1$.

(3) 导出矛盾: 由 G 非循环, 据例 7.3, G 中必存在两个不共轭的极大子群 M_1, M_2. 我们设

$$|M_1| = m_1, |G:M_1| = n_1, |M_2| = m_2, |G:M_2| = n_2.$$

由 (1) 和 (2) 有

$$\begin{aligned} \left| \bigcup_{g \in G} (M_1^g - \{1\}) \right| &= n_1(m_1 - 1) = |G| - n_1 \\ &= |G| - \frac{|G|}{m_1}. \end{aligned}$$

同理有

$$\begin{aligned} \left| \bigcup_{g \in G} (M_2^g - \{1\}) \right| &= n_2(m_2 - 1) = |G| - n_2 \\ &= |G| - \frac{|G|}{m_2}. \end{aligned}$$

再由 (2),

$$\left(\bigcup_{g\in G}(M_1^g-\{1\})\right)\cap\left(\bigcup_{g\in G}(M_2^g-\{1\})\right)=\varnothing.$$

故

$$\begin{aligned}|G|-1 &\geq \left|\bigcup_{g\in G}(M_1^g-\{1\})\right|+\left|\bigcup_{g\in G}(M_2^g-\{1\})\right| \\ &= 2|G|-\frac{|G|}{m_1}-\frac{|G|}{m_2}.\end{aligned}$$

于是有

$$|G|\leq\frac{|G|}{m_1}+\frac{|G|}{m_2}-1.$$

但 $m_1\geq 2, m_2\geq 2$, 故

$$|G|\leq\frac{|G|}{m_1}+\frac{|G|}{m_2}-1\leq\frac{|G|}{2}+\frac{|G|}{2}-1=|G|-1,$$

矛盾. □

例 7.11 (Zassenhaus 定理) 设 G 是有限群, 对于它的每个交换子群 A 恒有 $N_G(A)=C_G(A)$. 则 G 必为交换群.

证 首先我们注意到, 定理的条件是*子群遗传的*. 即对 G 的任一子群 M 以及 M 的任一交换子群 A, 也有 $N_M(A)=C_M(A)$. 这因为 $N_M(A)=N_G(A)\cap M=C_G(A)\cap M=C_M(A)$.

下面我们用分析极小反例的方法来证明定理的结论. 即假定定理不真, 并设 G 是使定理的结论不成立的最小阶群. 我们设法通过分析 G 的结构来导出矛盾, 从而建立定理的正确性.

设 G 是极小反例. 因为定理的条件是子群遗传的, 故由 G 的极小性, 定理的结论对它的每个真子群皆成立. 即它的每个真子群皆交换, 但 G 本身不交换. 根据例 7.10, G 中必存在非平凡正规子群. 我们在它的所有非平凡正规子群中选择一个极大的, 设其为 N, 则 G/N 是单群. 明显地, G/N 的每个真子群作为交换群的商

群当然也是交换群. 于是再用例 7.10 结论的逆否命题, 推出 G/N 必交换. 但它又是单群. 于是只能是素数阶循环群. 另一方面, N 作为 G 的真子群是交换群, 由定理假设, $C_G(N) = N_G(N) = G$, 即 $N \leq Z(G)$. 据 §2 习题 5, 得 G 交换, 最终得到了矛盾. □.

上面两题中所使用的方法, 即反证法和分析极小反例的方法 (后者的实质是反证法和归纳法的结合) 是初等有限群论中最基本的证明方法, 希望读者认真体会, 力争尽快掌握它们.

例 7.12 设 p 是奇素数. 令

$$G = \left\{ \begin{pmatrix} x & 0 \\ y & 1 \end{pmatrix} \middle| x, y \in GF(p),\ x \neq 0 \right\}.$$

则 G 对于矩阵乘法构成一个完全群.

证 设 r 是模 p 的原根. 又设

$$a = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, b = \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}.$$

则容易验证 $G = \langle a, b \rangle$, 且有定义关系

$$a^p = 1, b^{p-1} = 1, b^{-1}ab = a^r.$$

因为 $\langle a \rangle \trianglelefteq G$, 且 $(|\langle a \rangle|, |G : \langle a \rangle|) = 1$, 故 $\langle a \rangle$ char G. (参看 §2 末习题 2.) 现在设 $\alpha \in \mathrm{Aut}(G)$, 则 α 被 a, b 的像 a^α, b^α 所唯一确定. 由于 $\langle a \rangle$ char G, 有 $a^\alpha = a^i$, $p \nmid i$. 我们设 $b^\alpha = b^j a^k$, 则由 $b^{-1}ab = a^r$, 用 α 作用两边就得到 $(b^\alpha)^{-1} a^\alpha b^\alpha = (a^\alpha)^r$ 即

$$(b^j b^k)^{-1} a^i (b^j a^k) = a^{ir}.$$

由计算得 $a^{ir^j} = a^{ir}$, $a^{ir(r^{j-1}-1)} = 1$. 于是

$$ir(r^{j-1} - 1) \equiv 0 \pmod p,$$

$$r^{j-1} \equiv 1 \pmod p.$$

由 r 是模 p 的原根，有 $j-1\equiv 0 \pmod{p-1}$, $j\equiv 1 \pmod{p-1}$. 因此可设 $b^\alpha = ba^k$. 这样， a^α 最多有 $p-1$ 种可能性，而 b^α 最多有 p 种可能性. 于是得 $|\mathrm{Aut}(G)|\le p(p-1)$.

另一方面，容易验证 $Z(G)=1$, 于是内自同构群 $\mathrm{Inn}(G)\cong G$, 推出 $|\mathrm{Inn}(G)|=|G|=p(p-1)$. 这就迫使 $\mathrm{Aut}(G)\cong\mathrm{Inn}(G)$. 于是 G 是完全群. □

在这个例子中， G 实际上是素数阶循环群 Z_p 的全形. 这样就告诉我们，素数阶循环群的全形也是完全群，它们是可解完全群的又一个例子.

习 题

1. 设有限群 G 的每个真子群皆为交换群，则 G 是可解群.

2. 设有限群 G 的每个极大子群皆正规，且为单群，则 G 是交换群，并且 $|G|=p^2$ 或 pq, 其中 p, q 是素数.

3. 设

$$G=\left\{\begin{pmatrix} x & 0\\ y & 1\end{pmatrix}\middle|\, x,y\in Z_8, \text{且 } x \text{ 为可逆元}\right\}.$$

则 G 为 2^5 阶群. 并且映射

$$\alpha:\begin{pmatrix} x & 0\\ y & 1\end{pmatrix}\mapsto\begin{pmatrix} x & 0\\ y+\frac{1}{2}(x^2-1) & 1\end{pmatrix}$$

是 G 的一个外自同构，但它把 G 的每个共轭类都变到自身.

第 II 章

群在集合上的作用及其应用

本章首先引进群在集合上作用的概念，然后应用它证明有限群最重要的定理之一 ——Sylow 定理，继而再应用 Sylow 定理对 p-群和可解群做初步的研究. 这些构成了本章的前半部分. 本章的后半部分则应用群作用的思想研究群的置换表示以及群到子群的转移映射，证明了重要的 Burnside 定理. 同时给出了大量的应用它们判定有限群是否可解的例题.

我们认为，为掌握初等有限群论的证明方法和技巧，必须深刻理解并熟练运用群在集合上作用的观点，并且学会应用 Sylow 定理和置换表示 (包括转移映射) 这两个具有基本意义的结果和方法. 读者不仅应该彻底弄清本章中讲述的基本定理和结果，而且应该仔细研究分散在各节中的大量的由浅入深的例题，特别是关于群的可解性和非单性的例题. 只有这样，读者才能逐步掌握初等有限群论的基本方法，并且积累足够多的技巧，为今后进一步学习打下牢固的基础. 另一方面，通过研究这些例题，也使我们看到初等方法的局限性. 于是又自然而然地要求建立新的更强有力的方法. 这就是群表示论，局部分析方法以及几何的和组合的方法，它们在本书的下册将有初步的介绍.

§1. 群在集合上的作用

定义 1.1 设 $\Omega = \{\alpha, \beta, \gamma, \ldots\}$ 是一个非空集合，其元素称作点. S_Ω 表示 Ω 上的对称群. 所谓群 G 在 Ω 上的一个作用 φ 指

的是 G 到 S_Ω 内的一个同态. 即对每个元素 $x\in G$, 对应 Ω 上的一个变换 $\varphi(x):\alpha\mapsto\alpha^x$, 并且满足

$$(\alpha^x)^y=\alpha^{xy},\quad x;y\in G,\alpha\in\Omega;$$

或者

$$\varphi(xy)=\varphi(x)\varphi(y),\quad x,y\in G.$$

如果 $\mathrm{Ker}\ \varphi=1$, 则称 G**忠实地**作用在 Ω 上，这时可把 G 看作 Ω 上的变换群. 而如果 $\mathrm{Ker}\ \varphi=G$, 则称 G**平凡地**作用在 Ω 上.

命题 1.2 *设群 G 作用在集合 Ω 上，则对每个 $\alpha\in\Omega$,*

$$G_\alpha=\{x\in G\mid\alpha^x=\alpha\}$$

是 G 的子群，叫做点 α 的 **稳定子群**. *并且对任意的 $y\in G$, 有 $G_{\alpha^y}=y^{-1}G_\alpha y$.*

证　设 $x,y\in G_\alpha$, 则 $\alpha^x=\alpha$, $\alpha^y=\alpha$. 于是 $\alpha^{x^{-1}}=\alpha$, $\alpha^{xy}=\alpha^y=\alpha$, 即 $x^{-1}\in G_\alpha$, $xy\in G_\alpha$, 所以 $G_\alpha\le G$.

又，$x\in G_{\alpha^y}\iff(\alpha^y)^x=\alpha^y\iff\alpha^{yxy^{-1}}=\alpha\iff yxy^{-1}\in G_\alpha\iff x\in y^{-1}G_\alpha y$. 于是 $G_{\alpha^y}=y^{-1}G_\alpha y$. □

定义 1.3 设群 G 作用于集合 Ω 上，称二元素 $\alpha,\beta\in\Omega$ 为**等价的**, 记作 $\alpha\sim\beta$, 如果存在 $x\in G$, 使 $\alpha^x=\beta$. 易验证关系 "$\sim$" 是 Ω 上的等价关系. Ω 对 "$\sim$" 的一个等价类叫做 G 在 Ω 上的一个**轨道** (**传递集**). 一个轨道所包含的元素个数叫做该轨道的**长**.

对于 $\alpha\in\Omega$, 令

$$\alpha^G=\{\alpha^x\mid x\in G\},$$

则 α^G 是 G 的包含点 α 的轨道.

定义 1.4 如果 G 在 Ω 上只有一个轨道，即 Ω 本身，则称 G 在 Ω 上的作用是**传递的**. 这时也称 G 所对应的 Ω 上的变换群是传递的.

定理 1.5 设有限群 G 作用在有限集合 Ω 上, $\alpha \in \Omega$, 则

$$|\alpha^G| = |G : G_\alpha|.$$

特别地, 轨道 α^G 的长是 $|G|$ 的因子.

证 对任意的 $g \in G$, 规定 $f(g) = \alpha^g$. 则 f 是 G 到 α^G 上的满射. 因为对任意的 $g, h \in G$, 有

$$\begin{aligned} f(g) = f(h) \quad &\Longleftrightarrow \quad \alpha^g = \alpha^h \Longleftrightarrow \alpha^{gh^{-1}} = \alpha \\ &\Longleftrightarrow \quad gh^{-1} \in G_\alpha \Longleftrightarrow G_\alpha g = G_\alpha h. \end{aligned}$$

于是轨道 α^G 中不同点的个数恰为 G_α 在 G 中的右陪集个数. 即

$$|\alpha^G| = |G : G_\alpha|.$$

□

这个定理虽然简单, 但它是群作用的最基本的结果, 必须做到能熟练运用.

下面举几个群作用的例子, 除了应根据定义检验其确为群作用之外, 还应弄清它的稳定子群和轨道, 以及定理 1.5 在其中的涵义. 这些例子虽然简单, 但都是群作用的基本例子, 并且在今后经常要用到.

例 1.6 设 G 是群. 取 $\Omega = G$. G 在 Ω 上的作用为 $\varphi(x) : g \mapsto x^{-1}gx$, $\forall x, g \in G$. 这时作用的核 $\operatorname{Ker}\varphi = Z(G)$, 即群 G 的中心, 而对于 Ω 中的一点 g, 稳定子群 $G_g = C_G(g)$. 作用的轨道即群 G 的共轭元素类. 由任意二轨道之交为空集得诸共轭元素类互不相交. 这就得到群的类方程

$$|G| = \sum_i |C_i|,$$

其中 C_i 跑遍 G 的一切共轭元素类. 又, 定理 1.5 就给出 I,1.24 的前半部分.

例 1.7 设 G 是群. 取 $\Omega = 2^G$, 即 G 的所有子集所组成的集合. G 在 Ω 上的作用仍为共轭变换, 即 $\varphi(x) : H \mapsto x^{-1}Hx$, $\forall H \in 2^G, \forall x \in G$. 这时, 作用的核 $\mathrm{Ker}\,\varphi$ 仍为群的中心 $Z(G)$, 而点 H 的稳定子群为 H 在 G 中的正规化子 $N_G(H)$. 定理 1.5 在这种情形下就变成 I,1.24 的后半部分.

例 1.8 设 G 是群, $H \le G$. 取 $\Omega = \{Hg \mid g \in G\}$ 为 H 的全体右陪集的集合. 我们如下规定 G 在 Ω 上的一个作用 P:

$$P(x) : Hg \mapsto Hgx, \quad \forall Hg \in \Omega.$$

这时作用 P 的核 $\mathrm{Ker}\,P = \bigcap_{g\in G} g^{-1}Hg$, 即包含在 H 中的 G 的极大正规子群. 这个子群我们叫做 *H 在 G 中的核*, 记作 H_G 或 $\mathrm{Core}_G(H)$. 又, 任一点 Hg 的稳定子群 $G_{Hg} = g^{-1}Hg$, 特别地, $G_H = H$. 还应注意, 这个作用是传递作用, 即 G 在 Ω 上只有一个轨道, 即 Ω 本身. 对于这个例子, 在本章 §4 还要详细地研究.

定理 1.9 (Frattini 论断) *设 G 作用在 Ω 上, 并且 G 包含一个子群 N, 它在 Ω 上的作用是传递的, 则*

$$G = G_\alpha N, \quad \forall \alpha \in \Omega.$$

证　任取 $g \in G$, 并设 $\alpha^g = \beta$. 由 N 在 Ω 上传递, 存在 $n \in N$ 使 $\alpha^n = \beta$. 于是 $\alpha^{gn^{-1}} = \alpha$, 即 $gn^{-1} \in G_\alpha$. 由此得

$$g = (gn^{-1})n \in G_\alpha N.$$

□

§2. Sylow 定理

Lagrange 定理告诉我们, 若 G 是有限群, H 是 G 的子群, 则 $|H|$ 是 $|G|$ 的因子. 但反过来, 若 $d \mid |G|$, G 中是否一定存在 d 阶子群呢? 一般来说, 这是不对的. 例如, 交错群 A_4 是 12 阶

群，但它没有 6 阶子群．（这可如下证明：假定 A_4 有 6 阶子群 H，则因 A_4 中有 8 个 3 阶元，3 个 2 阶元和一个单位元，推出 H 中必有 3 阶元，从而有 3 阶子群 K. 又据 I,1.18, H 中 3 阶子群必唯一，于是 H 中恰有两个 3 阶元．这样，A_4 中的三个 2 阶元必都属于 H. 但它们和单位元组成 4 阶子群，而 Lagrange 定理即得到 $4 \mid 6$, 矛盾.）但是，Sylow 定理告诉我们，如果 $d \mid |G|$, d 是素数的方幂，则 G 中必有 d 阶子群存在.

在抽象代数课程中，我们已经学过 Sylow 定理．那时我们把它们总结成以下的三个定理：

第一 Sylow 定理: *若 G 是有限群，p 是素数．设 $p^n \parallel |G|$, 即 $p^n \mid |G|$, 但 $p^{n+1} \nmid |G|$. 则 G 中必存在 p^n 阶子群，叫做 G 的 Sylow p-子群.*

第二 Sylow 定理: *G 的任意二个 Sylow p-子群皆在 G 中共轭.*

第三 Sylow 定理: *G 中 Sylow p-子群的个数 n_p 是 $|G|$ 的因子，并且 $n_p \equiv 1 \pmod p$.*

在本节中，我们将从群作用的观点出发再给 Sylow 定理一个证明.

回忆一下，我们称一个群为 p-群，如果它的每个元素都是 p-元素，即阶为 p 的方幂的元素．又，我们称有限群的极大 p-子群为 Sylow p-子群．当我们证明了 Sylow 定理以后就可以看出，Sylow p-子群的这个定义和抽象代数中所学的定义是一致的.

我们先来证明

定理 2.1 *设 p 是素数，群 G 的阶为 $p^a n$, 这里不要求 p 和 n 互素．以 $n(p^a)$ 表示 G 中 p^a 阶子群的个数，则有 $n(p^a) \equiv 1 \pmod p$. 特别地有 $n(p^a) \geq 1$, 即 G 中存在 p^a 阶子群.*

证 (Wielandt) 设

$$\Omega = \{M \subseteq G \mid |M| = p^a\}$$

是 G 的所有包含 p^a 个元素的子集的集合，显然有 $|\Omega| = \binom{p^a n}{p^a}$. 规定

$$M^g = Mg, \quad M \in \Omega, \quad g \in G,$$

则 G 作用于集合 Ω 上. 这时 Ω 可表成 G 的诸轨道 T_i 的并. 如果 G 一共有 k 个轨道，则有

$$|\Omega| = \sum_{i=1}^{k} |T_i|.$$

在第 i 个轨道 T_i 中任取一代表元 M_i, 设 N_i 是 M_i 的稳定子群，即 $N_i = \{g \in G \mid M_i g = M_i\}$, 则有 $|T_i| = |G : N_i|$. 下面我们证明

(i) N_i 的阶为 p 的方幂：由 N_i 的定义可知，子集 M_i 和 N_i 的积 $M_i N_i = M_i$, 故 M_i 为 N_i 的若干个左陪集的并. 于是 $|N_i| \mid |M_i| = p^a$, 即得 $|N_i| = p^b \le p^a$.

(ii) 若 $|N_i| < p^a$, 则 $|T_i| \equiv 0 \pmod{pn}$; 而若 $|N_i| = p^a$, 则 $|T_i| = n$. 并且反过来也对. 因此得

$$|\Omega| \equiv \sum_{|T_i|=n} |T_i| \pmod{pn}.$$

(iii) G 在 Ω 上的长度为 n 的轨道个数等于 G 中 p^a 阶子群的个数 $n(p^a)$：设 T_i 是一长为 n 的轨道，M_i 是其中的任一元素. 则 M_i 的稳定子群 N_i 是 p^a 阶子群，并且有 $M_i = m_i N_i$, 对任一 $m_i \in M_i$ 成立. 而且还有

$$\begin{aligned} T_i &= \{M_i g \mid g \in G\} = \{M_i m_i^{-1} g \mid g \in G\} \\ &= \{m_i N_i m_i^{-1} g \mid g \in G\}. \end{aligned}$$

令 $H_i = m_i N_i m_i^{-1}$, 则 H_i 为 G 中 p^a 阶子群，并且有

$$T_i = \{H_i g \mid g \in G\}.$$

这说明，每个长为 n 的轨道都是某个 p^a 阶子群的全体右陪集的集合. 反过来，对任一 p^a 阶子群 H, 它的全体右陪集的集合

$T = \{Hg \mid g \in G\}$ 显然也为 G 在 Ω 上的一个长为 n 的轨道. 这就得到了 G 的长为 n 的轨道和 G 的 p^a 阶子群之间的一个一一对应, 由此即得所需之结论.

(iv) $|\Omega| \equiv n(p^a) \cdot n \pmod{pn}$: 把 (iii) 的结论代入 (ii) 中的同余式立得.

(v) $|\Omega| \equiv n \pmod{pn}$: 考虑 $p^a n$ 阶循环群 C, 它只有一个 p^a 阶子群, 但它的 p^a 元子集个数和 G 的一样, 也是 $|\Omega|$. 因为 (iv) 的结论对任意群都成立, 应用到循环群 C, 即得结论 (v).

至此可以完成定理的证明. 由 (iv) 和 (v) 得到 $n(p^a) \cdot n \equiv n \pmod{pn}$, 应用同余式的简单性质即得 $n(p^a) \equiv 1 \pmod{p}$. □

由这个定理首先可以推出, 有限 p-群 G 的阶必有 p 的方幂. 这因为若有素数 $q \neq p$, $q \mid |G|$, 则由定理 2.1 推出 G 中有 q 阶子群, 因而有 q 阶元素, 与 G 是 p-群矛盾. 另外, 这个定理包含了 Sylow 第一定理和 Sylow 第三定理为它的特例.

下面我们再证明

定理 2.2 *设 G 是有限群, $p^a \parallel |G|$. 再设 P 是 G 的一个 p^a 阶子群, Q 是 G 的任一 p-子群, 则必存在 $g \in G$ 使 $Q \le P^g$.*

证 考虑 G 关于子群 P, Q 的双陪集分解

$$G = Pg_1Q \cup Pg_2Q \cup \cdots \cup Pg_kQ.$$

每个 Pg_iQ 中所包含的 P 的右陪集个数为 $|Q|/|P^{g_i} \cap Q|$, 故为 p 的方幂. 但因 $|G:P|$ 与 p 互素, 故至少存在一个 i 使 $|Q|/|P^{g_i} \cap Q| = 1$, 即 $|Q| = |P^{g_i} \cap Q|$, 于是 $Q \le P^{g_i}$. 取 $g = g_i$, 即得所需之结论. □

这个定理告诉我们, 每个 p-子群都属于一个 p^a 阶子群. 这就推出 G 中的极大 p-子群必为 p^a 阶的. 也就是说, 我们以极大 p-子群作为有限群的 Sylow p-子群的定义和前面第一 Sylow 定理中叙述的 Sylow p-子群的定义是一致的. 另外, 在定理 2.2 中, 取 Q 为另一 p^a 阶子群, 就得到所有 Sylow 子群的共轭性. 即定理 2.2 包含第二 Sylow 定理为其特例.

下面列出关于有限群的 Sylow p-子群的几个简单但十分有用的结论，其证明请读者自行补足. 为了方便起见，我们以 $\mathrm{Syl}_p(G)$ 表示有限群 G 的所有 Sylow p-子群的集合，于是 $P \in \mathrm{Syl}_p(G)$ 就表示 P 是 G 的 Sylow p-子群. 又令 $n_p(G) = |\mathrm{Syl}_p(G)|$, 即 G 中 Sylow p-子群的个数. 在不至引起混淆的情况下，常把 $n_p(G)$ 简记作 n_p.

命题 2.3 设 G 是有限群，则

(1) 若 $P \in \mathrm{Syl}_p(G)$, $P \leq H \leq G$, 则 $P \in \mathrm{Syl}_p(H)$;

(2) 若 $H \leq G$, $R \in \mathrm{Syl}_p(H)$, 则存在 $P \in \mathrm{Syl}_p(G)$ 使 $R = P \cap H$;

(3) 若 $P \in \mathrm{Syl}_p(G)$, B 是任一 p-子群，并满足 $PB = BP$, 则 $B \leq P$. 特别地，若 Q 是 G 的正规 p-子群，则 Q 含于 G 的任一 Sylow p-子群之中；

(4) G 的所有 Sylow p-子群的交，记作 $O_p(G)$, 是 G 的极大正规 p-子群，它包含 G 的每个正规 p-子群，并且 $O_p(G)$ char G;

(5) 若 $P \in \mathrm{Syl}_p(G)$, 且 $P \trianglelefteq G$, 则 $n_p(G) = 1$, 并且 P char G. 特别地，P 是 $N_G(P)$ 中唯一的 Sylow p-子群；

(6) 若 $N \trianglelefteq G$, $P \in \mathrm{Syl}_p(G)$, 则 $P \cap N \in \mathrm{Syl}_p(N)$, $PN/N \in \mathrm{Syl}_p(G/N)$;

(7) 若 $P \in \mathrm{Syl}_p(G)$, $\alpha \in \mathrm{End}(G)$, 则 $P^\alpha \in \mathrm{Syl}_p(G^\alpha)$.

下面再叙述几个与 Sylow 子群有关的结果，它们在有限群中十分重要.

定理 2.4 (Frattini 论断) 设 $N \trianglelefteq G$, $P \in \mathrm{Syl}_p(N)$, 则 $G = N_G(P)N$.

证　令 $\Omega = \mathrm{Syl}_p(N)$. G 依共轭变换作用在 Ω 上. 由第二 Sylow 定理，N 在 Ω 上传递. 又，P 的稳定子群 $G_P = N_G(P)$. 于是由定理 1.9 得

$$G = G_P N = N_G(P)N.$$

□

命题 2.5 设 $P \in \mathrm{Syl}_p(G)$, $H \geq N_G(P)$, 则 $H = N_G(H)$.

证 因为 $H \trianglelefteq N = N_G(H)$, 并且 P 也是 H 的 Sylow p-子群, 由定理 2.4, $N = H \cdot N_N(P) \leq H \cdot N_G(P) \leq H$, 于是有 $N = H$. □

命题 2.6 设 P 是 G 的任一 p-子群, $N \trianglelefteq G$, 且 $(|N|, p) = 1$. 则 $N_{G/N}(PN/N) = N_G(P)N/N$.

证 考虑 G 到 G/N 的自然同态, 由第一同构定理, $M/N \trianglelefteq G/N$ 等价于 $M \trianglelefteq G$, 于是 $N_G(PN)/N = N_{G/N}(PN/N)$. 故只需证 $N_G(PN) = N_G(P)N$.

显然, $N_G(P) \leq N_G(PN)$, $N \leq N_G(PN)$, 故 $N_G(P)N \leq N_G(PN)$. 又若 $x \in N_G(PN)$, 则 $P^x \leq PN$. 因 $(|N|, p) = 1$, P 和 P^x 皆为 PN 之 Sylow p-子群, 故存在 $h \in P, n \in N$ 使 $P^x = P^{hn} = P^n$. 由此得 $P = P^{xn^{-1}}$, 即 $xn^{-1} \in N_G(P)$, $x \in N_G(P)n \subseteq N_G(P)N$. 这又得到相反的包含关系 $N_G(PN) \leq N_G(P)N$. 于是有 $N_G(PN) = N_G(P)N$. □

§3. 可解群和 p-群

Sylow 定理是有限群最基本的结果之一. 本节通过介绍可解群和 p-群的若干初等结果来讲述 Sylow 定理的应用.

定理 3.1 *设 G 是有限群, P 是 G 的 p-子群, 但不是 Sylow p-子群. 则 $P < N_G(P)$.*

证 考虑 G 对子群 P, P 的双陪集分集

$$G = \bigcup_{i=1}^{k} Px_iP.$$

每个 Px_iP 中含 P 的右陪集的个数为 $|P|/|P^{x_i} \cap P|$, 是 p 的方幂. 又因 $p \mid |G:P|$, 而 $P1P = P$ 仅含一个 P 的右陪集, 故至少还有 $x_i \notin P$, 使 Px_iP 仅含一个 P 的右陪集. 对于这个 x_i, 必有 $P^{x_i} \cap P = P$, 于是 $P^{x_i} = P$. 这就得出 $P < N_G(P)$. □

回忆一下，我们称 M 为群 G 的*极大子群*，如果 $M < G$，并且由 $M \leq K \leq G$ 可推得 $K = M$ 或 $K = G$.

推论 3.2 *设 M 是有限 p-群 G 的极大子群，则 $|G : M| = p$，且 $M \trianglelefteq G$.*

证　因 $M < G$，M 自然不是 G 的 Sylow p-子群．由定理 3.1 得 $M < N_G(M)$．又由 M 的极大性得 $N_G(M) = G$，即 $M \trianglelefteq G$．再考虑 G/M．仍由 M 之极大性知 G/M 没有非平凡子群，于是 G/M 是 p 阶循环群，$|G : M| = p$.　□

定理 3.3 *有限 p-群 G 是可解群.*

证　设 $|G| = p^n$，用对 n 的归纳法．当 $n = 0$ 时结论显然成立．现设结论对 $n-1$ 成立，来考察 n 的情形．任取 G 的极大子群 M，由推论 3.2，$|M| = p^{n-1}$，于是 M 是可解群．又 G/M 为 p 阶循环群，亦可解，故由命题 I,4.13(1)，得 G 可解.　□

下面再应用 Sylow 定理给出可解性的几个充分条件.

定理 3.4 *设 p, q 是素数，则 pq 阶群 G 是可解群.*

证　不妨假定 $p < q$．设 Q 是 G 的 Sylow q-子群，则 $|Q| = q$，且 Q 的共轭子群个数为 $kq+1$，这时有 $kq + 1 \mid p$．由 $p < q$，得 $k = 0$，于是 G 仅有一个 Sylow q-子群，由第二 Sylow 定理，$Q \trianglelefteq G$．又因 $|G/Q| = p$，$|Q| = q$，知 G/Q 和 Q 均可解，于是 G 可解.　□

定理 3.5 *设 p, q 是素数，a 是正整数，则 $p^a q$ 阶群可解.*

证　用归纳法，只需证明 G 中存在非平凡正规子群.

设 P 是 G 的 Sylow p-子群．可假定 $P \ntrianglelefteq G$，并设 $P = P_1, \ldots, P_s$ 是 G 的全部 Sylow p-子群．由 $s \mid q$ 及 $s > 1$ 推出 $s = q$．下面分两种情形来讨论：

(i) 设对任意的 $i \neq j$，$P_i \cap P_j = 1$．于是 $\bigcup_{i=1}^{q} P_i$ 包含 $(p^a - 1)q + 1$ 个元素．此外还只剩下 $q - 1$ 个元素．因 G 中存在 q 子群，故只能有一个 q 阶子群，这样它必为正规子群.

(ii) 若有 $P_i \cap P_j > 1$. 选 $i, j, i \neq j$, 使 $|P_i \cap P_j|$ 最大. 令 $P_i \cap P_j = D$. 因 $D < P_i$, 故 $D < N_{P_i}(D) = H_i \leq P_i$. 又因 $D < P_j$, 有 $D < N_{P_j}(D) = H_j \leq P_j$. 这时有 $D \trianglelefteq \langle H_i, H_j \rangle = T$.

1) 设 T 是 p-子群. 则存在 G 的 Sylow p-子群 P_k 使 $T \leq P_k$. 由 $P_k \cap P_i \geq H_i > D$, $P_k \cap P_j \geq H_j > D$ 以及 D 的选择的极大性推得 $P_k = P_i$, $P_k = P_j$, 于是 $P_i = P_j$, 矛盾. 因此必有

2) $|T| = p^t q$. 令 Q 是 T 的 q 阶子群, 由 I,1.18, 比较阶易知 $G = QP_i$. 设 $N = D^G$, 则有 $N \trianglelefteq G$. 我们证明 N 必为 G 之真子群, 从而完成了证明. 这因为对任意的 $g \in G$, 可设 $g = xy$, 其中 $x \in Q$, $y \in P_i$. 所以 $D^g = D^{xy} = D^y \leq P_i$, 于是 $D^G \leq P_i < G$, 证毕. □

定理 3.6 设素数 $p > q > r$, 则 pqr 阶群 G 是可解群.

证 设 G 中有 n_p 个 p 阶子群, n_q 个 q 阶子群和 n_r 个 r 阶子群. 注意到上述子群均为 G 的 Sylow 子群, 如果 n_p, n_q, n_r 均不为 1, 由 Sylow 定理, 必有 $n_p > p, n_q > q, n_r > r$, 以及 $n_p \mid qr$, $n_q \mid pr$, $n_r \mid pq$. 于是必有 $n_p = qr$, $n_q \geq p$, $n_r \geq q$. 因此,

G 中 p 阶元个数 $= n_p(p-1) = qr(p-1) = pqr - qr$,

G 中 q 阶元个数 $= n_q(q-1) \geq p(q-1) = pq - p$,

G 中 r 阶元个数 $= n_r(r-1) \geq q(r-1) = qr - q$.

于是有

$$\begin{aligned} |G| &\geq 1 + pqr - qr + pq - p + qr - q \\ &= |G| + (p-1)(q-1), \end{aligned}$$

矛盾. 故 n_p, n_q, n_r 中至少有一个是 1. 比如设 $n_p = 1$. 这推出 p 阶子群 $P \trianglelefteq G$, 而 G/P 是 qr 阶群, 由定理 3.4, G/P 可解. 于是 G 亦可解. □

在本章 §5, 我们将把这个定理推广为: 只要 G 的所有 Sylow 子群皆循环, 则 G 可解 (推论 5.6).

另外, Burnside 的下述著名定理推广了 3.5,

定理 3.7 (Burnside) 设 p, q 是素数， a, b 是正整数，则 $p^a q^a$ 阶群必可解.

这个定理常被称为 Burnside $p^a q^b$ 定理．我们将在第 VI 章给它一个表示论的证明，并在下册的第 VIII 章 §6, 给出一个纯粹群论的证明.

另一个最著名的可解性判定定理是

定理 3.8 (Feit-Thompson) 奇数阶群必可解.

欲知这个定理的证明，目前还只能够研读 Feit 和 Thompson 的长达 255 页的原始证明，载 *Pacific J. Math.*, **13**(1963), 775-1029. (尽管 G. Glauberman 和 D. Sibley 已给出长约 150 页的简化证明，但目前尚未发表). 由于这个定理的证明如此复杂，一般在初等群论中尽量避免使用它．但下面我们应用这个定理来证明一个新的可解性准则.

定理 3.9 设 $|G| = 2n$, n 是奇数，则 G 必可解.

证　由 Sylow 定理， G 中必存在 2 阶元素 u. 考虑 G 的右正则表示 $R(G)$. (见定理 I, 3.12 的证明). u 所对应的右乘变换 $R(u)$ 也是 2 阶元，故 $R(u)$ 为若干个互不相交的对换的乘积．又由 $R(u)$ 的定义，易知 $R(u)$ 无不动点，因此 $R(u)$ 可表成 n 个对换的乘积．于是 $R(u)$ 是奇置换，即我们证明了 $R(G)$ 中含有奇置换．这推出 $R(G)$ 中所有偶置换组成指数为 2 的正规子群 N, $|N| = n$ 是奇数．由 3.8, N 可解．又 $R(G)/N$ 是 2 阶群，亦可解，于是 $R(G)$ 可解．而 $G \cong R(G)$, 这就得到 G 的可解性. □

用此方法还可证明，只要有限群 G 的 Sylow 2-子群循环，则 G 必可解，把这作为习题留给读者.

以下我们转入对有限 p-群的讨论．首先证明 p-群的两个最基本的性质，然后给出阶 $\leq p^3$ 的所有有限 p-群的完全分类．这部分内容虽与群的可解性无关，但因其方法也是典型的，且其结果以后经常用到，放在这里来叙述是合适的.

定理 3.10 设 G 是有限 p-群，$|G| = p^n > 1$，则 $Z(G) > 1$.

证 考虑 G 的共轭类分解

$$G = C_1 \cup C_2 \cup \cdots \cup C_s, \quad C_1 = \{1\},$$

和类方程

$$|G| = 1 + |C_2| + \cdots + |C_s|.$$

因为 $|C_i| = |G : C_G(x_i)|$，其中 $x_i \in C_i$，由 $|G| = p^n$ 推知 $|C_i|$ 是 p 的方幂. 又由 $|C_1| = 1$ 推知至少还有某个 $|C_i| = 1$，于是 $Z(G) > 1$. □

定理 3.11 设 G 是有限 p-群，N 是 G 的 p 阶正规子群，则 $N \le Z(G)$.

证 由 N/C 定理，

$$G/C_G(N) = N_G(N)/C_G(N) \lesssim \mathrm{Aut}(N).$$

因 $\mathrm{Aut}(N)$ 是 $p-1$ 阶循环群，而 $|G/C_G(N)|$ 是 p 的方幂，故 $|G/C_G(N)| = 1$，即 $G = C_G(N)$，$N \le Z(G)$. □

下面我们来决定所有阶 $\le p^3$ 的 p-群.

首先，p 阶群必为循环群，只有一种类型. 而对 p^2 阶群，有下面的

定理 3.12 p^2 阶群 G 必为交换群.

证 若 G 中有 p^2 阶元素，则 G 为 p^2 阶循环群. 若 G 中无 p^2 阶元素，则它的每个非单位元都是 p 阶元. 根据定理 3.10，$Z(G) > 1$. 取 $a \in Z(G)$，$a \neq 1$，则 $\langle a \rangle$ 是 $Z(G)$ 中的 p 阶子群. 再取 $b \notin \langle a \rangle$，则 $G = \langle a, b \rangle$. 由 $a \in Z(G)$，$ab = ba$，故 G 为交换群. □

由此定理及 I,4.7，p^2 阶群有两种类型，即型不变量为 (p^2) 和 (p, p) 的交换群.

现在来决定 p^3 阶群. 首先由 I,4.7, p^3 阶交换群有三种类型, 其型不变量分别为 (p^3), (p^2, p) 和 (p, p, p). 下面研究非交换情形.

设 G 是 p^3 阶非交换群. 任取 p 阶正规子群 N, 则因 $|G/N| = p^2$, G/N 是交换群, 得 $N \geq G'$. 但 $G' \neq 1$, 则必有 $N = G'$, 并且 $G' \leq Z(G)$. 再注意到 G 中必无 p^3 阶元素, 我们可分下面两种情形:

(1) G 中有 p^2 阶元素 a: 这时 $\langle a\rangle$ 是 G 的极大子群. 因此 $\langle a\rangle \trianglelefteq G$. 因 $\langle a^p\rangle$ char $\langle a\rangle$, 故 $\langle a^p\rangle \trianglelefteq G$. 由前面的分析知 $G' = \langle a^p\rangle$. 在 $\langle a\rangle$ 外面任取一元 b_1, 再分两种情形:

(i) $o(b_1) = p$: 因为 $G = \langle a, b_1\rangle$, 换位子 $[a, b_1] \neq 1$, 但因 $G' = \langle a^p\rangle$, 故可设 $[a, b_1] = a^{kp}$, 这里 $p \nmid k$. 取 i 满足 $ik \equiv 1 \pmod p$, 令 $b = b_1^i$, 则由第 I 章 §4 习题 9 有 $[a, b] = [a, b_1^i] = [a, b_1]^i = a^{ikp} = a^p$, 于是 G 有关系

$$a^{p^2} = b^p = 1, \quad b^{-1}ab = a^{1+p}. \tag{I}$$

(ii) $o(b_1) = p^2$: 因为 $b_1^p \in \langle a\rangle$, 比较阶可令 $b_1^p = a^{kp}$. 如果 $p \neq 2$, 则由第 I 章 §4 习题 9 有

$$(b_1a^{-k})^p = b_1^p a^{-kp}[a, b_1^{-k}]^{\binom{p}{2}} = 1,$$

知 $\langle a\rangle$ 外有 p 阶元 b_1a^{-k}, 因此化为情形 (i). 而如果 $p = 2$, 则可能有 $b_1^2 = a^2$, $[a, b_1] = a^2$. 这时以 b 代 b_1, 得 G 有下述关系:

$$a^4 = 1, \quad b^2 = a^2, \quad b^{-1}ab = a^3. \tag{II}$$

(2) G 中无 p^2 阶元素: 区别 $p = 2$ 和 $p \neq 2$ 两种情形.

若 $p = 2$, 由 $\exp G = 2$ 推出 G 交换, 即非交换群不会发生此种情形.

若 $p \neq 2$, 假定 $G/G' = \langle aG', bG'\rangle$, 于是 $G = \langle a, b, G'\rangle$. 但由 G 非交换, 必有 $[a, b] \neq 1$. 于是 $G' = \langle [a, b]\rangle$, 并且还有 $G = \langle a, b\rangle$. 令 $c = [a, b]$, 这时 G 有关系

$$a^p = b^p = c^p = 1, \quad [a, b] = c, \quad [a, c] = [b, c] = 1. \tag{II$'$}$$

应用第 I 章 §6 的知识，读者可自行验证以 (I), (II), (II′) 为定义关系的群确为 p^3 阶非交换群，并且它们互不同构，于是它们就是全部的 p^3 阶非交换群.

总结一下，p^3 阶非交换群 $G = \langle a, b\rangle$ 有下列类型：

(A) $p = 2$

(I) $a^4 = b^2 = 1, \quad b^{-1}ab = a^3$; (二面体群)

(II) $a^4 = 1, \quad b^2 = a^2, b^{-1}ab = a^3$. (四元数群)

(B) $p \neq 2$

(I) $a^{p^2} = b^p = 1, \quad b^{-1}ab = a^{1+p}$;

(II′) $a^p = b^p = c^p = 1, \quad [a,b] = c, \quad [a,c] = [b,c] = 1$.

§4. 传递置换表示及其应用

所谓群的置换表示指的是群到置换群中的同态. 如果同态像是传递置换群，则称为传递置换表示. 例 1.8 给出了有限群 G 的传递置换表示的例子，即对任一子群 $H \leq G$, 取 Ω 为 H 的所有右陪集的集合，作用 P 取右乘变换. 我们称 P 为 G**在子群** H **上的置换表示**, 并简记成

$$P(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}, \qquad g \in G.$$

该表示的核 $\operatorname{Ker} P = H_G$, 为子群 H 在 G 中的核. 因此有 $P(G) \cong G/H_G$.

下面我们要证明，事实上这个例子就穷尽了全部的传递置换表示. 为此先引进

定义 4.1 设置换群 $G_1 \leq S_{\Omega_1}$, $G_2 \leq S_{\Omega_2}$. 若存在一一映射 $\mu : \Omega_1 \to \Omega_2$ 和一一映射 $\sigma : G_1 \to G_2$, 使

$$\mu g_1^{\sigma} = g_1\mu, \qquad \forall g_1 \in G_1,$$

则称 G_1 和 G_2**置换同构**.

注意，在此定义中给出的映射 σ 一定是群 G_1 到 G_2 的同构，这因为

$$(g_1g_1')^\sigma = \mu^{-1}g_1g_1'\mu = \mu^{-1}g_1\mu\mu^{-1}g_1'\mu = g_1^\sigma g_1'^\sigma,\ \forall g_1, g_1' \in G.$$

(这里，μ^{-1} 是 μ 的逆映射，它是 Ω_2 到 Ω_1 的一一映射.)

定理 4.2 *设 φ 是有限群 G 在 Ω 上的传递作用. 则存在子群 $H \le G$, 使得 $\varphi(G)$ 与 G 在 H 上的置换表示 $P(G)$ 置换同构.*

证　任取 $\alpha \in \Omega$, 令 $H = G_\alpha$. 对于 Ω 中任一元素 β, 由 $\varphi(G)$ 传递，存在 $g_\beta \in G$ 使 $\alpha^{g_\beta} = \beta$, 则

$$G = \bigcup_{\beta\in\Omega} Hg_\beta,$$

并且若 $\beta \neq \gamma$, 则 $Hg_\beta \neq Hg_\gamma$. 这样得到 Ω 到 $\{Hg \mid g \in G\}$ 的一一映射 $\mu : \beta \mapsto Hg_\beta$. 则 $(\alpha^g)^\mu = Hg$, $\forall g \in G$. 再令 $\sigma : \varphi(g) \mapsto P(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}$, 易验证 σ 也是一一映射. (验证略.) 并且对任意的 $\beta \in \Omega$, 有

$$\begin{aligned} \beta^{\mu\varphi(g)^\sigma} &= \beta^{\mu P(g)} = Hg_\beta g, \\ \beta^{\varphi(g)\mu} &= (\alpha^{g_\beta})^{\varphi(g)\mu} = (\alpha^{g_\beta g})^\mu = Hg_\beta g, \end{aligned}$$

因此 $\mu\varphi(g)^\sigma = \varphi(g)\mu$. 这就得到 $\varphi(G)$ 与 $P(G)$ 置换同构. □

以下我们再引进同一群 G 的两个置换表示等价的概念.

定义 4.3 设 $\varphi_1 : G \to S_{\Omega_1}$ 和 $\varphi_2 : G \to S_{\Omega_2}$ 是群 G 的两个置换表示. 若存在一一映射 $\mu : \Omega_1 \to \Omega_2$ 使 $\mu\varphi_2(g) = \varphi_1(g)\mu$, $\forall g \in G$, 则称此二置换表示**等价**.

定理 4.4 *设 G 是群，$H, K \le G$. 再设 P_1, P_2 分别是 G 在 H, K 上的置换表示:*

$$P_1(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix},\ P_2(g) = \begin{pmatrix} Kx \\ Kxg \end{pmatrix},\ \forall g \in G.$$

则 P_1, P_2 等价 $\iff$ H, K 在 G 中共轭.

证 $\Leftarrow$: 设 H,K 共轭, $K=H^y, y\in G$. 令

$$\mu: Hx\mapsto Ky^{-1}x,\quad x\in G,$$

则易验证 μ 是 $\Omega_1=\{Hx \mid x\in G\}$ 到 $\Omega_2=\{Kx \mid x\in G\}$ 上的一一映射. 并且由

$$(Hx)^{\mu P_2(g)}=Ky^{-1}xg=(Hxg)^{\mu}=(Hx)^{P_1(g)\mu},$$

得到 $\mu P_2(g)=P_1(g)\mu, \forall g\in G$. 于是 P_1,P_2 等价.

$\Rightarrow$: 设 P_1,P_2 等价. 假定 μ 是定义 4.3 中要求的 $\Omega_1=\{Hx \mid x\in G\}$ 到 $\Omega_2=\{Kx \mid x\in G\}$ 的一一映射, 并设在 μ 之下 Hx 对应到 Ky. 由 P_1,P_2 的等价性, 点 Hx 在 $P_1(G)$ 中的稳定子群等于点 Ky 在 $P_2(G)$ 中的稳定子群, 即 $x^{-1}Hx=y^{-1}Ky$. 于是得 H,K 的共轭性. □

注意: P_1,P_2 等价与置换群 $P_1(G)$ 和 $P_2(G)$ 置换同构是有区别的. P_1,P_2 等价实际上是要求 $P_1(g)\mapsto P_2(g)$ 是定义 4.1 中的映射 σ, 但作为置换群的置换同构, 映射 σ 并无此限制. (可参看本章末习题 8.)

就置换表示对抽象群的应用而言, 下列命题是十分重要的.

命题 4.5 设 $H\le G$, $|G:H|=n$, 则 $|G/H_G|$ 是 $(n!,|G|)$ 的因子.

证 考虑 G 在 H 上的置换表示 P, 有

$$G/\mathrm{Ker}\ P=G/H_G\cong P(G)\lesssim S_n,$$

由此即得所需之结论. □

下面举几个应用置换表示的例子.

命题 4.6 设 G 是有限群, p 是 $|G|$ 的最小素因子. 又设 $H\le G$, 且 $|G:H|=p$, 则 $H\trianglelefteq G$.

证 由命题 4.5, $|G/H_G| \mid (p!, |G|) = p$. 这就迫使 $H_G = H$, 即 $H \trianglelefteq G$. □

定理 4.7 60 阶单群必同构于 A_5.

证 考虑 60 阶单群 G 的传递置换表示. 由于 G 是单群, 每个置换表示都是忠实的. 因此 G 不能有到 S_n, $n \leq 4$, 中的置换表示. 这说明 G 中不存在指数 ≤ 4 的子群.

下面证明 G 中存在指数为 5, 即 12 阶的子群. 根据 Sylow 第三定理, G 中 Sylow 2-子群的个数 $n_2 = 3, 5$ 或 15. 因为 n_2 是 Sylow 2-子群的正规化子的指数, 前面已证 G 中无指数为 3 的子群, 故 n_2 只能为 5 或 15. 若 $n_2 = 5$, 则 G 中已有指数为 5 的子群. 若 $n_2 = 15$, 又假定 G 的任二 Sylow 2-子群之交均为 1, 则 G 的 2-元素共有 $1 + 3 \times 15 = 46$ 个. 而由 Sylow 定理, G 的 Sylow 5-子群的个数 $n_5 = 6$, 非单位的 5-元素个数为 $4 \times 6 = 24$. 于是 2-元素与 5-元素总数已超过群阶, 故不可能. 这说明必有 G 的二个 Sylow 2-子群之交为 2 阶群 A. 考虑 A 的中心化子 $C_G(A)$. 它已含有两个 Sylow 2-子群, 故其阶 > 4, 并且是 4 的倍数. 但前面已证 G 中没有指数 ≤ 4 的子群, 于是推出 $|C_G(A)| = 12$.

设 H 是 G 的任一 12 阶子群, 则 G 在 H 上的置换表示使 G 同构于 S_5 的 60 阶子群. 但 S_5 中只有一个 60 阶子群, 即 A_5, 故得 $G \cong A_5$. □

例 4.8 144 阶群 G 不可能为单群.

证 因 $144 = 2^4 \cdot 3^2$, 由 Sylow 定理, $n_3(G) = 4$ 或 16, 设 $P \in \mathrm{Syl}_3(G)$. 若 $n_3 = 4$, 则 $|G : N_G(P)| = 4$. 若令 $N_G(P)$ 的核为 C, 考虑 G 在 $N_G(P)$ 上的传递置换表示, 可得 $G/C \lesssim S_4$, 即 C 为 G 的非平凡正规子群, G 非单. 而若 $n_3 = 16$, 再分两种情形: (1) 假定任二 Sylow 3-子群之交为 1, 则 G 的 3-元素个数为 $16 \times (9-1) + 1 = 129$ 个. 这推出 G 中 2-元素个数至多为 $144 - 129 + 1 = 16$ 个. 但 G 中有 16 阶子群, 即 Sylow 2-子群, 这就说明 Sylow 2-子群必唯一, 它是 G 的非平凡正规子群.

(2) 存在两个 Sylow 3-子群，其交为 $D > 1$. 这时必有 $|D| = 3$. 令 $H = N_G(D)$. 则 H 至少包含 G 的两个 Sylow 3-子群, 即 $n_3(H) > 1$. 但由 Sylow 定理，有 $n_3(H) \geq 4$, $|H| = n_3(H) \cdot |N_H(P)| \geq 4 \cdot 3^2$, 于是 $|G : H| \leq 4$. 若 $H = G$, 则 $D \trianglelefteq G$, D 是 G 的非平凡正规子群; 而若 $H < G$, 则由命题 4.5, $|G/H_G| \bigm| 4!$, 于是 H_G 是 G 的非平凡正规子群. □

为了研究下一个例子，我们需要关于 Sylow 子群个数的一个更为精细的结果. 即本章末的习题 16. 在这里我们仅对习题中 $d = 2$ 的情形来叙述并证明这个结果.

命题 4.9 *设 G 的 Sylow p-子群的个数 $n_p(G) \not\equiv 1 \pmod{p^2}$, 则必存在 G 的二 Sylow p-子群 P_1, P_2 使得 $|P_1 : P_1 \cap P_2| = p$.*

证 用反证法. 假定结论不真，即对任二个 Sylow p-子群 P_i, P_j, 均有 $|P_i : P_i \cap P_j| \geq p^2$. 再设 $P_0, P_1, \ldots, P_s$ 为 G 之全部不同的 Sylow p-子群. 考虑 P_0 依共轭变换在集合 $\Omega = \{P_1, \ldots, P_s\}$ 上的作用. 因为对任意的 $x \in P_0$, $i \geq 1$, $P_i^x \neq P_0$, 故这确为 P_0 在 Ω 上的作用. 又，Ω 中任一点 P_i 的稳定子群为 $N_G(P_i) \cap P_0$. 我们要证 $N_i = N_G(P_i) \cap P_0 = P_i \cap P_0$. 显然只须证 $N_i \leq P_i \cap P_0$. 因 N_i 正规化 P_i, 故 $N_iP_i = P_iN_i$. 由命题 2.3(3), 得 $N_i \leq P_i$, 当然有 $N_i \leq P_i \cap P_0$. 现在应用定理 1.5, 包含点 P_i 的轨道的长为 $|P_0 : N_i| = |P_0 : P_i \cap P_0| \geq p^2$, 于是 P_0 在 Ω 上作用的每个轨道长皆为 p^2 的倍数，这就推出 $n_p(G) = s + 1 \equiv 1 \pmod{p^2}$, 与假设矛盾. □

例 4.10 不存在 $432 = 2^4 \cdot 3^3$ 阶单群.

证 由 Sylow 定理，432 阶群 G 的 Sylow 3-子群个数 $n_3 = 4$ 或 16. 若 $n_3 = 4$, 则 G 有指数为 4 的子群. 由命题 4.5, 知 G 非单群. 而若 $n_3 = 16$, 则因 $16 \not\equiv 1 \pmod{3^2}$, 知必存在 G 的二 Sylow 3-子群 P_1, P_2 使 $|P_1 : P_1 \cap P_2| = 3$. 于是由定理 3.1, $N_G(P_1 \cap P_2) \geq P_i$, $i = 1, 2$. 这推出 $|N_G(P_1 \cap P_2)| \geq 4 \cdot 3^3$. 于是，或者 $P_1 \cap P_2 \trianglelefteq G$,

或者 G 中存在指数 ≤ 4 的真子群. 无论哪种情形都推出 G 非单群. □

为了讲述群的置换表示的进一步应用, 我们在本节末尾先来研究一下置换表示中元素和子群的不动点的性质, 然后在下节末尾结合 Burnside 定理的应用再讲几个例题.

命题 4.11 *设 G 是有限群, $P \in \mathrm{Syl}_p(G)$, $N = N_G(P)$, $\Omega = \{Ng \mid g \in G\}$. 再设 φ 是 G 在子群 N 上的置换表示, 则 $\varphi(P)$ 在 Ω 上只有一个不动点 N.*

证 因为 $NP = N$, 故 N 是 $\varphi(P)$ 的不动点. 若 $\varphi(P)$ 又有不动点 Nx, $x \notin N$. 则由 $Nx = NxP$ 推出 $N = N(xPx^{-1})$, 于是 $xPx^{-1} \leq N$. 但 N 中只有一个 Sylow p-子群 P, 故 $xPx^{-1} = P$, 由此得 $x \in N_G(P) = N$, 矛盾. □

上述命题的一个特殊情形是下面的

推论 4.12 *设 G 是有限群, $P \in \mathrm{Syl}_p(G)$, $|P| = p$, $N = N_G(P)$. 又设 φ 是 G 在 N 上的置换表示, $1 \neq x \in P$, 则 $\varphi(x)$ 的轮换分解式由一个 1-轮换和若干个 p-轮换组成.*

命题 4.13 *设 G, P, N, φ 同推论 4.12. 又设 k 是 $\varphi(P)$ 的轨道数, $x \in N_G(P) - C_G(P)$. 则 $\varphi(x)$ 的不动点数至多为 k.*

证 若否, 则至少有 $\varphi(x)$ 的两个不动点 Na, Nb 属于 $\varphi(P)$ 的同一轨道. 因为 N 是 $\varphi(P)$ 的不动点, 它们都不能是 N. 于是有 $Nax = Na$, $Nbx = Nb$, $ab^{-1} \notin N$, 并且存在 $1 \neq y \in P$ 使 $Nay = Nb$. 这推出 $Na(yxy^{-1}x^{-1}) = Na$, 即 Na 是 $\varphi(yxy^{-1}x^{-1})$ 的不动点. 又因 $x \in N_G(P)$, $y \in P$, 则 $yxy^{-1}x^{-1} \in P$. 于是 N 也是 $\varphi(yxy^{-1}x^{-1})$ 的不动点. 由命题 4.11, $\varphi(P)$ 只有一个不动点 N. 再由 $|P| = p$, 若 $yxy^{-1}x^{-1} \neq 1$, 则 $\varphi(yxy^{-1}x^{-1})$ 也只有一个不动点 N, 这就迫使 $yxy^{-1}x^{-1} = 1$, 即 $x \in C_G(y) = C_G(P)$, 与 x 的选择矛盾. □

§5. 转移和 Burnside 定理

设 G 是有限群 [1], $H \le G$. 令

$$G = \bigcup_{i=1}^{n} Hx_i$$

是右陪集分解式. 我们以 P 记 G 在 H 上的置换表示. 设 $g \in G$, 则 $P(g) = \begin{pmatrix} Hx_i \\ Hx_ig \end{pmatrix}$. 假定

$$Hx_ig = Hx_{i^{\tau(g)}}, \quad i = 1, 2, \ldots, n,$$

则 $\tau(g)$ 是集合 $\{1, 2, \ldots, n\}$ 的一个置换, 而 τ 可看成是 G 到对称群 S_n 内的同态映射. 现在令 $x_ig = h_i(g)x_{i^{\tau(g)}}$, $h_i(g) \in H$, 则

$$h_i(g) = x_igx_{i^{\tau(g)}}^{-1} \in H.$$

定义 5.1 所谓 G 到 H 内的 **转移** 指的是 G 到 H/H' 内的映射 $V_{G\to H}$, 满足

$$V_{G\to H}(g) = \prod_{i=1}^{n} h_i(g)H', \quad g \in G.$$

注意, 由这个定义, 为了决定映射 $V_{G\to H}$, 先须取定 H 在 G 中的一组右陪集代表系 $\{x_i\}$.

命题 5.2 (1) $V_{G\to H}$ 是 G 到 H/H' 内的同态;

(2) $V_{G\to H}$ 不依赖于 H 的陪集代表的选取;

(3) 设 $K \le H \le G$, $g \in G$. 如果 $V_{G\to H}(g) = hH'$, 那么 $V_{G\to K}(g) = V_{H\to K}(h)$.

证 (1) 若 $g_1, g_2 \in G$, 则

$$V_{G\to H}(g_1g_2) \quad = \quad \prod_{i=1}^{n} h_i(g_1g_2)H'$$

[1] 对于无限群 G 的子群 H, 也可同样定义转移映射, 并且命题 5.2 也成立.

$$
\begin{aligned}
&= \prod_{i=1}^{n} x_i g_1 g_2 x_{i^{\tau(g_1 g_2)}}^{-1} H' \\
&= \prod_{i=1}^{n} x_i g_1 x_{i^{\tau(g_1)}}^{-1} x_{i^{\tau(g_1)}} g_2 x_{i^{\tau(g_1)\tau(g_2)}}^{-1} H' \\
&= \prod_{i=1}^{n} x_i g_1 x_{i^{\tau(g_1)}}^{-1} H' \prod_{i=1}^{n} x_{i^{\tau(g_1)}} g_2 x_{i^{\tau(g_1)\tau(g_2)}}^{-1} \\
&= \prod_{i=1}^{n} h_i(g_1) H' \prod_{i=1}^{n} h_{i^{\tau(g_1)}}(g_2) H' \\
&= V_{G\to H}(g_1)\cdot V_{G\to H}(g_2),
\end{aligned}
$$

故 $V_{G\to H}$ 是同态.

(2) 再取一组陪集代表 $\{y_i\}$, 其中 $y_i \in Hx_i$. 这时有 $G = \bigcup_{i=1}^{n} Hy_i$. 令 $y_i = t_i x_i$, $t_i \in H$. 对于 $g \in G$, 再令 $y_i g = k_i(g) y_{i^{\tau(g)}}$, $k_i(g) \in H$. 于是 $k_i(g) = y_i g y_{i^{\tau(g)}}^{-1}$. 用这组陪集代表得到的转移映射暂记为 $\tilde{V}_{G\to H}$, 则有

$$
\begin{aligned}
\tilde{V}_{G\to H}(g) &= \prod_{i=1}^{n} k_i(g) H' = \prod_{i=1}^{n} y_i g y_{i^{\tau(g)}}^{-1} H' \\
&= \prod_{i=1}^{n} t_i x_i g x_{i^{\tau(g)}}^{-1} t_{i^{\tau(g)}}^{-1} H' \\
&= \prod_{i=1}^{n} t_i H' \prod_{i=1}^{n} h_i(g) H' \prod_{i=1}^{n} t_{i^{\tau(g)}}^{-1} H' \\
&= \prod_{i=1}^{n} h_i(g) H' \\
&= V_{G\to H}(g).
\end{aligned}
$$

于是 $\tilde{V}_{G\to H} = V_{G\to H}$, 即转移映射不依赖于陪集代表的选取.

(3) 设 $G = \bigcup_{i=1}^{n} Hx_i$ 和 $H = \bigcup_{j=1}^{m} Ky_j$ 分别为 G 对于 H 和 H 对于 K 的右陪集分解式, 则 $G = \bigcup_{i,j} Ky_j x_i$ 是 G 对 K 的右陪集分解.

对于任意的 $h \in H$, 设 $y_j h = k_j(h) y_{j^{\sigma(h)}}$, 其中 $k_j(h) \in K$, σ 是由 H 在 K 上的置换表示得到的 H 到 S_m 中的同态. 于是有

$$\begin{aligned} y_j x_i g &= y_j h_i(g) x_{i^{\tau(g)}} \\ &= k_j(h_i(g)) y_{j^{\sigma(h_i(g))}} x_{i^{\tau(g)}}. \end{aligned}$$

现在令 $V_{G\to H}(g) = hH'$, 于是 $hH' = \prod_{i=1}^n h_i(g)H'$, 由此推出

$$\prod_{i=1}^n h_i(g) = hh',$$

其中 $h' \in H'$. 由计算可得

$$\begin{aligned} V_{G\to K}(g) &= \prod_{i=1}^n \prod_{j=1}^m k_j(h_i(g))K' \\ &= \prod_{i=1}^n V_{H\to K}(h_i(g)) \\ &= V_{H\to K}(\prod_{i=1}^n h_i(g)) \\ &= V_{H\to K}(hh') \\ &= V_{H\to K}(h) \cdot V_{H\to K}(h') \\ &= V_{H\to K}(h). \end{aligned}$$

最后一步是因为 K/K' 是交换群, 同态 $V_{H\to K}$ 的核包含 H', 于是有 $V_{H\to K}(h') = K'$. □

因为映射 $V_{G\to H}$ 不依赖于 H 的陪集代表系的选取, 在计算 $V_{G\to H}(g)$ 时, 为了使表达式简单, 可如下选 H 的陪集代表: 把 $P(g)$ 写成不相交轮换的乘积, 可设其轮换分解式为

$$P(g) = \prod_{i=1}^t (Hx_i, Hx_i g, \cdots, Hx_i g^{f_i - 1}),$$

即 $P(g)$ 可表成 t 个轮换的乘积, 诸轮换的长度分别为 $f_1, f_2, \cdots, f_t$, 有 $\sum_{i=1}^t f_i = |G:H|$. 并且因 $Hx_i g^{f_i} = Hx_i$, 有 $x_i g^{f_i} x_i^{-1} \in H$; 但当

$f < f_i$ 时, $x_i g^f x_i^{-1} \notin H$. 我们就把 $x_i, x_i g, \cdots, x_i g^{f_i - 1}, i = 1, \cdots, t$, 取作陪集代表. 利用这组代表元计算转移映射有

$$\begin{aligned} V_{G \to H}(g) &= \prod_{i=1}^{t} x_i \cdot g(x_i g)^{-1} \cdot x_i g \cdot g(x_i g^2)^{-1} \cdots x_i g^{f_i - 1} \cdot g x_i^{-1} H' \\ &= \prod_{i=1}^{t} x_i g^{f_i} x_i^{-1} H'. \end{aligned} \tag{5.1}$$

应用转移映射的最典型的例子之一是下面的 Burnside 定理. 为叙述这个定理, 我们先引进下面的概念.

定义 5.3 设 G 是有限群, $P \in \mathrm{Syl}_p(G)$. 如果 G 有正规子群 N, 满足 $N \cap P = 1$, $NP = G$, 则称 G 为 p-幂零群, 而称 N 为 G 的 正规 p-补.

显然, 正规子群 N 是 G 的正规 p-补的充要条件为 $|N| = |G||P|^{-1}$, 其中 $P \in \mathrm{Syl}_p(G)$.

定理 5.4 (Burnside) *设 G 是有限群, $P \in \mathrm{Syl}_p(G)$. 若 $N_G(P) = C_G(P)$, 则 G 为 p-幂零群.*

证 因为 $C_G(P) = N_G(P) \geq P$, 知 P 为交换群. 考虑转移映射 $V_{G \to P}$. 若能证明 $V_{G \to P}(G) = P$, 则由同态基本定理知 $\mathrm{Ker}\, V_{G \to P}$ 就是 G 的正规 p-补, 于是 G 是 p-幂零群.

事实上我们可以证明 $V_{G \to P}(P) = P$. 设 $1 \neq g \in P$. 由 (5.1) 式, 并注意到 $P' = 1$, 有

$$V_{G \to P}(g) = \prod_{i=1}^{t} x_i g^{f_i} x_i^{-1}.$$

因为 g^{f_i} 和 $x_i g^{f_i} x_i^{-1}$ 均属于 P, 由 P 的交换性有 $C_G(g^{f_i}) \geq P$, $C_G(x_i g^{f_i} x_i^{-1}) \geq P$. 由后式又推出 $x_i C_G(g^{f_i}) x_i^{-1} \geq P$, 即 $C_G(g^{f_i}) \geq x_i^{-1} P x_i$. 这样, 在 $C_G(g^{f_i})$ 中有两个 (不一定不同的) G 的 Sylow p-子群 P 和 $x_i^{-1} P x_i$. 据 Sylow 定理, 存在 $u \in C_G(g^{f^i})$ 使

$u^{-1}Pu = x_i^{-1}Px_i$. 于是 $x_iu^{-1} \in N_G(P) = C_G(P) \le C_G(g^{f_i})$, 故 $x_i \in C_G(g^{f_i})$, 即 $x_ig^{f_i}x_i^{-1} = g^{f_i}$. 这样

$$V_{G\to P}(g) = \prod_{i=1}^{t} x_ig^{f_i}x_i^{-1} = \prod_{i=1}^{t} g^{f_i} = g^{|G:P|}.$$

因为 $(p, |G:P|) = 1$, 由 $g \ne 1$ 就得到 $V_{G\to P}(g) \ne 1$. 这说明 $V_{G\to P}$ 限制在 P 上是 P 到 P 的单射. 由 P 有限, 当然也是满射. 因此有 $V_{G\to P}(P) = P$. □

关于转移和 p-幂零群的进一步研究可见第 VIII 章. 下面我们给出 Burnside 定理的若干应用.

定理 5.5 设 p 是 $|G|$ 的最小素因子, $P \in \mathrm{Syl}_p(G)$, 且 P 循环, 则 G 有正规 p-补.

证 由 N/C 定理, $N_G(P)/C_G(P) \lesssim \mathrm{Aut}(P)$. 设 $|P| = p^n$, 由 P 循环, 有 $|\mathrm{Aut}(P)| = \varphi(p^n) = p^{n-1}(p-1)$. 但因 $P \le C_G(P)$ 有 $p \nmid |N_G(P)/C_G(P)|$. 根据 p 的最小性, 必有 $|N_G(P)/C_G(P)| = 1$, 即 $N_G(P) = C_G(P)$. 应用 Burnside 定理, 即得 G 的 p-幂零性. □

推论 5.6 设有限群 G 的所有 Sylow 子群均为循环群, 则 G 是可解群.

证 设 $|G| = p_1^{\alpha_1}\cdots p_s^{\alpha_s}$, 其中 $p_1 < \cdots < p_s$. 用对 s 的归纳法, 由定理 5.5, G 有正规 p_1-补 N, 满足 $G/N \cong P_1 \in \mathrm{Syl}_{p_1}(G)$. 于是 $|N| = p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, 且 N 的 Sylow 子群也都循环. 由归纳假设, 得 N 的可解性. 又由 P_1 可解, 得 G 可解. □

定理 5.7 设 G 是有限非交换单群, p 是 $|G|$ 的最小素因子. 则 $p^3 \mid |G|$ 或 $12 \mid |G|$.

证 设 $p^3 \nmid |G|$, 则由定理 5.5 及 G 的单性, 必有 $p^2 \parallel |G|$ 且 G 的 Sylow p-子群 P 为 (p,p) 型初等交换 p-群. 这时有 $|\mathrm{Aut}(P)| = (p^2-1)(p^2-p) = (p-1)^2p(p+1)$. 令 $A = N_G(P)/C_G(P)$, 由 N/C

定理，$A \lesssim \mathrm{Aut}(P)$. 又由 P 交换，有 $C_G(P) \geq P$, 于是 $p \nmid |A|$. 再由 p 的最小性，有 $|A| \mid (p+1)$. 假定 $|A| = 1$, 即 $N_G(P) = C_G(P)$, 由 Burnside 定理得 G p-幂零，矛盾于 G 的单性，故 $|A| > p$. 只能有 $|A| = p+1$, 于是必有 $p = 2$, $|A| = 3$, 因此 $4 \cdot 3 = 12 \mid |G|$. □

下面的简单事实在确定一个群的非单性时十分有用.

定理 5.8 设 G 是有限非交换单群，$|G| = pm$, p 是素数，且 $(p, m) = 1$, 又设 $P \in \mathrm{Syl}_p(G)$, 则 $C_G(P) < N_G(P) < G$, 且 $|N_G(P)/C_G(P)| \mid p-1$.

证 由 G 是单群，$P \ntrianglelefteq G$, 有 $N_G(P) < G$. 又由 G 非 p-幂零及 Burnside 定理，有 $C_G(P) < N_G(P)$. 最后由 $N_G(P)/C_G(P) \lesssim \mathrm{Aut}(P)$, 以及 $|\mathrm{Aut}(P)| = p-1$, 有 $|N_G(P)/C_G(P)| \mid p-1$. □

下面再举几个应用 Burnside 定理来证明群的非单性的例子.

例 5.9 $3^3 \cdot 5 \cdot 7$ 阶群 G 必非单群.

证 设 G 是单群，$P \in \mathrm{Syl}_5(G)$. 由定理 5.8 有 $|N_G(P)/C_G(P)|$ 整除 $(5-1) = 4$, 因 $(4, |G|) = 1$, 必有 $|N_G(P)/C_G(P)| = 1$. 应用 Burnside 定理，得 G p-幂零，矛盾于 G 的单性. □

例 5.10 $2^2 \cdot 3^2 \cdot 11$ 阶群 G 必可解.

证 由 Sylow 定理，若 G 的 Sylow 11-子群 P 不正规，则 $n_{11}(G) = 12$, 于是 $|N_G(P)| = 3 \cdot 11 = 33$. 又由 N/C 定理，$N_G(P)/C_G(P) \lesssim \mathrm{Aut}(P)$. 因 $|\mathrm{Aut}(P)| = 10$, $(33, 10) = 1$, 故 $|N_G(P)/C_G(P)| = 1$, 即 $N_G(P) = C_G(P)$. 应用 Burnside 定理，G 有正规 11-补. 这说明 G 或有 11 阶正规子群，或有 36 阶正规子群. 再由 11 阶和 36 阶群的可解性即得 G 的可解性. □

定理 5.11 设 $|G| = p^2q^n$, $p < q$ 是素数，则 G 可解.

证 设 G 的 Sylow q-子群 $Q \ntrianglelefteq G$, 则 $n_q(G) = p^2$, 且 $q \mid p^2 - 1 = (p-1)(p+1)$. 由 $p < q$, 只能有 $p = 2$, $q = 3$, 于是

$|G:Q|=4$. 考虑 G 在 Q 上的置换表示, 推得 $G/Q_G \lesssim S_4$, 于是 G/Q_G 可解. 又 Q_G 是 q-群, 亦可解, 故得 G 的可解性. □

例 5.12 $2^3 \cdot 3^3 \cdot 5 = 1080$ 阶群 G 非单.

证 设 G 是单群. 由 $6! < 1080$, 应用命题 4.5, 推知 G 中不存在指数 ≤ 6 的子群. 由 Sylow 定理, G 中 Sylow 5-子群的个数 $n_5(G)=6, 36$ 或 216. 若 $n_5(G)=6$, 则 G 中有指数为 6 的子群; 若 $n_5(G)=216$, 则有 $N_G(P)=C_G(P)=P$, 其中 $P \in \mathrm{Syl}_5(G)$. 应用 Burnside 定理, G 有正规 5-补, 与 G 是单群矛盾. 故只能有 $n_5(G)=36$. 这时, $|N_G(P))|=30$. 又由 $N_G(P)/C_G(P) \lesssim \mathrm{Aut}(P) \cong Z_4$, $N_G(P) \neq C_G(P)$, 必有 $|C_G(P)|=15$. 易证 15 阶群必为循环群, 这样 $C_G(P)$ 循环. 设 H 是 $C_G(P)$ 中的 3 阶子群, 则由 H char $C_G(P)$, $C_G(P) \trianglelefteq N_G(P)$, 有 $H \trianglelefteq N_G(P)$. 再考虑 H 的正规化子 $N_G(H)$. 由定理 3.1, 有 $3^2 \mid |N_G(H)|$. 但因 $3^2 \nmid |N_G(P)|$, 必有 $N_G(P) < N_G(H)$. 于是, 在 $N_G(H)$ 中的 Sylow 5-子群的个数 $= |N_G(H):N_G(P)| > 1$. 据 Sylow 定理, 这个数或为 6, 或为 36. 若其为 36, 有 $N_G(H)=G$, 于是 $H \trianglelefteq G$; 而若其为 6, 则 $|G:N_G(H)|=6$, 与 G 中无指数 ≤ 6 的子群相矛盾. □

下面几个例题除了应用 Burnside 定理之外, 还要应用群的置换表示.

例 5.13 180 阶群 G 非单.

证 设 G 是单群. 因 $180 = 2^2 \cdot 3^2 \cdot 5$, 由 Sylow 定理, $n_5(G)=6$ 或 36. 若 $n_5(G)=36$, 则 $N_G(P)=C_G(P)=P$, 其中 $P \in \mathrm{Syl}_5(G)$. 由 Burnside 定理, G 有正规 5-补, 与 G 的单性矛盾, 于是必有 $n_5(G)=6$, 这时 $|N_G(P)|=30$. 由定理 5.8, $C_G(P) < N_G(P)$, 并且 $|N_G(P)/C_G(P)| \mid 4$, 于是必有 $|C_G(P)|=15$. 因 15 阶群皆循环, 故 G 中有 15 阶元素. 考虑 G 在 $N_G(P)$ 上的置换表示, 由 G 的单性, 表示是忠实的, 于是 $G \lesssim S_6$. 但容易看出 S_6 中无 15 阶元, 矛盾. □

例 5.14 $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$ 阶群 G 非单.

证 设 G 是单群. 由 Sylow 定理, $n_7(G) = 15$. 设 $P \in \mathrm{Syl}_7(G)$, 则 $|N_G(P)| = 28$. 由 Burnside 定理, 有 $C_G(P) < N_G(P)$. 又由 N/C 定理, $|N_G(P)/C_G(P)| \mid 7-1=6$, 于是必有 $|C_G(P)| = 14$. 这时 $C_G(P)$ 是 14 阶循环群. 取 14 阶元 $x \in C_G(P)$, 则 $x^2 \in P$, $o(x^2) = 7$. 考虑 G 在 $N_G(P)$ 上的忠实置换表示 φ, 则由推论 4.12, $\varphi(x^2)$ 是两个 7-轮换的乘积. 因 $\varphi(x^2) = \varphi(x)^2$, 故 $\varphi(x)$ 只能为一个 14-轮换. 这样 $\varphi(G)$ 中有奇置换 $\varphi(x)$. 因此 $\varphi(G)$ 中所有偶置换组成 $\varphi(G)$ 的指数为 2 的正规子群, 与 $\varphi(G)$ 的单性矛盾. □

例 5.15 $264 = 2^3 \cdot 3 \cdot 11$ 阶群 G 非单.

证 设 G 是单群. 由 Sylow 定理, $n_{11}(G) = 12$. 设 $P \in \mathrm{Syl}_{11}(G)$, 则 $|N_G(P)| = 22$, 由 Burnside 定理, $C_G(P) < N_G(P)$. 但因 $C_G(P) \geq P$, 故 $C_G(P) = P$. 取 $x \in N_G(P) - C_G(P)$. 考虑 G 在 $N_G(P)$ 上的忠实传递置换表示 φ. 由命题 4.11, $\varphi(P)$ 只有一个不动点, 于是 $\varphi(P)$ 有两个轨道. 再由命题 4.13, $\varphi(x)$ 的不动点数 ≤ 2. 另一方面, 因 $C_G(P) = P$, 知 $N_G(P)$ 非交换, 于是 $N_G(P)$ 中的 Sylow 2-子群个数为 11, 即 $N_G(P)$ 中有 11 个 2 阶元, 这说明在 $N_G(P) - C_G(P)$ 中的元素皆为 2 阶元, 于是 $o(x) = 2$, $o(\varphi(x)) = 2$. 又因 $\varphi(x)$ 至多有两个不动点, 以及 $x \in N_G(P)$, 又得到 $\varphi(x)$ 至少有一个不动点, 就推出 $\varphi(x)$ 是五个对换的乘积, 因而是奇置换. 和上例相同, $\varphi(G)$ 中有指数为 2 的正规子群, 矛盾于 G 的单性. □

习 题

1. 设 G 是群, α, β 是 G 的自同态. 规定

$$\varphi(g) : x \mapsto (g^{-1})^\beta x g^\alpha,$$

则 φ 是 G 在 G 上的一个作用.

2. 设 G 作用在 Ω 上, $H \leq G$, Σ 是 H 的轨道. 则对任意的 $x \in G$, Σ^x 是 $x^{-1}Hx$ 的轨道.

3. 设 G 在 Ω 上的作用是传递的，$N \trianglelefteq G$, 则 N 在 Ω 上所有轨道的长都相等.

4. 若交换群 G 忠实而传递地作用在 Ω 上，则 $G_\alpha = 1, \forall \alpha \in \Omega$. 特别地，有 $|G| = |\Omega|$.

5. 设有限群 G 忠实地作用在 Ω 上，A 是 G 的交换子群，它在 Ω 上的作用传递，则 $C_G(A) = A$.

6. 设 G 作用在 Ω 上，G 在 Ω 上的轨道个数为 t. 对于 $x \in G$, 令 x 的不动点集为

$$\mathrm{fix}_{\,\Omega}(x) = \{\alpha \in \Omega \mid \alpha^x = \alpha\}.$$

再令 $f_x = |\mathrm{fix}_{\,\Omega}(x)|$. 则 $t|G| = \sum_{x\in G} f_x$. 特别地，若 G 在 Ω 上传递，则有 $|G| = \sum_{x\in G} f_x$, 且当 $|\Omega| > 1$ 时，G 中必有正则元素，即没有不动点的元素.

7. 设有限群 G 传递地作用在 Ω 上，$\alpha \in \Omega$. 则 $N_G(G_\alpha)$ 也传递地作用在 $\Gamma = \{\beta \in \Omega \mid \beta^{G_\alpha} = \beta\}$ 上.

8. 设 P_1, P_2 分别是 G 在子群 H_1, H_2 上的置换表示，并且都是忠实的，则 $P_1(G)$ 和 $P_2(G)$ 置换同构的充要条件是存在 $\alpha \in \mathrm{Aut}(G)$ 使 $H_1^\alpha = H_2$.

9. 设 G 是有限群，$H \leq G$, $x \in H$, 以 $Cl(x)$ 表 x 所在的共轭元素类. 令 $f(x) = |Cl(x) \cap H|$. 再设 φ 是 G 在 Ω 上的置换表示，这里 $\Omega = \{Hg \mid g \in G\}$, 以 $\mathrm{fix}_{\,\Omega}(x)$ 表 $\varphi(x)$ 在 Ω 上的不动点集，则有

$$|Cl(x)| = \frac{|G:H|f(x)}{|\mathrm{fix}_{\,\Omega}(x)|}.$$

10. 验证 $GF(p)$ 上主对角线元素皆为 1 的 n 级上三角矩阵全体组成 $GL(n,p)$ 的一个 Sylow p-子群.

11. 若以 $|G|_p$ 表整除 $|G|$ 的 p 的最高次幂. 证明：假定 G 中存在 $|G|_p$ 阶子群 P, $H \leq G$, 则 H 中也存在 $|H|_p$ 阶子群 (不许用 Sylow 定理).

12. 结合 10,11 两题给出任意有限群 G 存在 $|G|_p$ 阶子群的一个证明.

13. 设 G 是有限交换群，$|G| = s$. 并令 $G = \{g_1, \ldots, g_s\}$. 设 $p \mid s$, 又设 $o(g_i) = n_i$, 则在形状为

$$g_1^{x_1} \cdots g_s^{x_s}, \quad 0 \leq x_i < n_i, \quad i = 1, \ldots, s$$

的诸乘积中，G 的每个元素出现的次数常相等，从而推出 G 中有 p 阶元素. 再用归纳法证明 G 中存在 $|G|_p$ 阶子群，即 Sylow p-子群.

14. 依下法给出有限群 G 存在 $|G|_p$ 阶子群的一个证明：设 G 是最小阶反例，则

(1) 设 $H < G$, 则 $p \mid |G:H|$;

(2) G 中不存在 $\neq 1$ 的正规 p-子群;

(3) 用 (1), (2), 类方程推出 $p \mid |Z(G)|$;

(4) 用 13 题推出矛盾.

15. 设 $|G| = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, $P_i \in \mathrm{Syl}_{p_i}(G)$, $i = 1, \ldots, s$. 则

(1) $G = \langle P_1, \ldots, P_s \rangle$;

(2) 若又有 $P_i \trianglelefteq G$, $i = 1, \ldots, s$, 则 $G = P_1 \times \cdots \times P_s$.

16. 设 $P_1 \ldots, P_n$ 是有限群 G 全部的 Sylow p-子群. 若对任意的 $i \neq j$ 总有 $|P_i : P_i \cap P_j| \geq p^d$, 则 $n \equiv 1 \pmod{p^d}$.

17. 设 G 是有限 p-群, 则 G 的非正规子群的个数是 p 的倍数.

18. 设有限群 G 的 Sylow 2-子群循环, 则 G 是可解群 (不用 Burnside 定理).

19. 设 p 是 $|G|$ 的最小素因子. 若 $N \trianglelefteq G$ 且 $|N| = p$, 则 $N \leq Z(G)$.

20. 设 p 是 $|G|$ 的最小素因子, 且 $p \neq 2$. 若 $N \trianglelefteq G$, 且 $|N| = p^2$, 则 $|G : C_G(N)| \leq p$.

21. (Brodkey) 设有限群 G 的 Sylow p-子群是交换群, 且所有 Sylow p-子群之交为 1, 则必有两个 Sylow p-子群, 它们的交也为 1.

22. 证明 2^3p^n 阶群 G 可解, 其中 $p > 2$ 是素数.

23. 设 $|G| = p^2q^2$, 证明 G 中存在正规 Sylow 子群.

24. 设 $|G| = p^2q^3$, 且 $p < q$, 证明 G 中存在正规 Sylow 子群. 但若 $p > q$, 则此结论不真.

25. 设 $|G| \leq 200$, 且 $|G| \neq 60, 120, 168, 180$, 则 G 可解.

26. 存在 $60, 120, 168, 180$ 阶非可解群, 但不存在 120, 180 阶单群.

27. 证明 $5 \cdot 7 \cdot 13$ 阶群必为循环群.

28. 设 n 是正整数, 证明所有 n 阶群皆循环的充要条件是 $(n, \varphi(n)) = 1$, 这里 $\varphi(n)$ 是 Euler φ 函数.

29. 设 p 是素数, G 是有限群, $p^2 \mid |G|$, 则 $p \mid |\mathrm{Aut}(G)|$.

30. 证明 1008 阶群 G 非单.

31. 设 $|G| = p^2qr$, 其中 p, q, r 为不同素数. 则 G 可解或 $G \cong A_5$.

第 III 章

群的构造理论初步

在学习了有限群几个最基本的定理和若干初等方法之后，我们转而研究有限群的构造理论.

代数学的基本问题之一就是决定由某些公理定义的代数系究竟有多少互不同构的类型，即所谓同构分类问题. 对于很多代数系来说，这个问题已经得到解决. 例如 Wedderburn 的环的构造定理，Frobenius 关于实数域上有限维可除代数的分类定理，Cartan 关于复数域上单 Lie 代数的分类定理等等. 最简单的，在学习线性代数时我们知道，任意域上给定维数的线性空间都彼此同构，这实际上就是域上有限维线性空间的同构分类定理. 它告诉我们，从同构的意义上来说，任意域上给定维数 n 的线性空间只有一个. 又比如，第 I 章定理 3.8 给出了有限和无限循环群的同构分类定理；而第 I 章 §4 则解决了有限交换群的同构分类问题，即证明了每个有限交换群都可分解为若干有限循环群的直积，并且其基元素的阶被该群唯一确定. 根据在那节中给出的一系列定理我们可以很容易地写出任意给定 n 阶的有限交换群的全部互不同构的类型. 再比如，在第 II 章 §3, 我们对任一素数 p 决定了所有 p 阶， p^2 阶和 p^3 阶群的互不同构的类型. 这些都可作为解决同构分类问题成功的例子.

基于同样的想法，A.Cayley 在给出了抽象群的公理化定义以后，于 1878 年明确地提出了对于一般的 n 阶有限群的同构分类问题. 和循环群以及交换群的情形迥然不同，人们发现这个问题是

惊人的复杂和困难. 前言中已经提到经过数百名数学家数十年的艰苦努力, 今天我们已经解决了有限单群的同构分类问题. 但距离解决 Cayley 提出的一般有限群的分类还十分遥远. 尽管如此, 近百年来, 我们总算得到了若干具有基本意义的有限群的构造定理, 诸如 Jordan-Hölder 定理, 直积分解定理, Schur-Zassenhaus 定理以及 Schreier 群扩张理论等. 它们为解决有限群的同构分类问题指出了方向并勾画了粗糙的轮廓. 本章的目的就是来讲述这些定理, 它们不仅对同构分类问题而且对有限群的整个理论来说都具有基本的意义. 附带地, 我们也来讲述几种由较小的群构造较大的群的方法. 在第 I 章中已经讲过的直积是最简单的一种, 本章中还要介绍半直积 (§3) 和圈积 (§5). 最后, 在 §6 我们介绍所谓 $\mathcal{P}$- 临界群的概念, 它是研究群的构造的一种重要的方法.

§1. Jordan-Hölder 定理

在开始抽象的讲述和颇为枯燥的逻辑推导之前, 我们先来介绍一下 Jordan-Hölder 定理 的基本想法.

设 G 是有限群. 若 G 有非平凡正规子群 N, 则可做商群 G/N. 从某种意义上来说, 我们可把 G 看成是由两个较小的群 N 和 G/N 合成的. (若用本章 §3 的术语, G 是 N 被 G/N 的扩张.) 假若 N 或 G/N 还有非平凡正规子群, 这种 "分解" 还可以继续下去. 因为 G 是有限群, 这个过程总可以进行到底, 即我们可以找到 G 的一个子群列.

$$G = G_0 > G_1 > G_2 > \ldots > G_{r-1} > G_r = 1,$$

其中 $G_i \trianglelefteq G_{i-1}, i = 1, \ldots, r$, 并且商群 G_{i-1}/G_i 都没有非平凡正规子群, 也就是说都是单群. 因此我们可以认为, G 是由诸单群 $G_{i-1}/G_i, i = 1, \ldots, r$, 合成的. Hölder 就把这样的群列叫做群 G 的 *合成群列*, 而把诸单群 G_{i-1}/G_i 叫做 G 的 *合成因子*.

这时自然发生一个问题: 群 G 的合成群列是否唯一? 如果不唯一, 又有哪些东西能被群 G 所唯一决定? Jordan-Hölder 定理就回答了这个问题. 它告诉我们, 尽管有限群 G 可以有不同的合

成群列，但它们的长度是唯一确定的，并且 (从同构的意义上来说) 诸合成因子，若不计次序，也被群 G 所唯一决定. 这很类似于正整数的素因子分解唯一性定理，即算术基本定理. 只要我们把群类比正整数，单群类比素数，合成群列类比正整数的一个素因子分解式. 我们知道，算术基本定理对算术来说具有基本的意义，因此可以想见 Jordan-Hölder 定理对有限群的重要意义.

类似于合成群列，我们还可定义群 G 的 *主群列*.

$$G = H_0 > H_1 > H_2 > \ldots > H_{s-1} > H_s = 1.$$

它满足：每个子群 H_i 都是 G 的正规子群，(不仅是 H_{i-1} 的正规子群)，而在 H_{i-1} 和 H_i 之间不能再插入 G 的另一正规子群. 亦即对 $i = 1, \ldots, s$, H_{i-1}/H_i 是 G/H_i 的极小正规子群. 对于主群列，我们仍可提出上述对合成群列提出的唯一性问题，Jordan-Hölder 定理对它给出了类似合成群列的肯定的回答.

为了给合成群列和主群列一个统一的处理，并得出更广的结论，我们先引进算子群的概念.

定义 1.1 (1) 设 G 是群，Ω 是一个集合. 对任一 $\alpha \in \Omega$, 指定一个群 G 的自同态：$g \mapsto g^\alpha$, $\forall g \in G$, 则称 G 为具有算子集 Ω 的算子群，或称 G 为一个 Ω- 群.

不改变问题的实质，我们还可改换成另一种说法：令 Ω 为 $\mathrm{End}(G)$ 的任一子集，称 (G, Ω) 为一个 Ω- 群.

(2) G 的子群 H 叫做 *可容许的*(或 Ω- 子群), 如果 $H^\alpha \le H$, $\forall \alpha \in \Omega$.

(3) 设 N 是 G 的可容许的正规子群 (或正规 Ω- 子群), 则在商群 G/N 中规定

$$(gN)^\alpha = g^\alpha N, \qquad g \in G, \qquad \alpha \in \Omega,$$

可使 G/N 成一 Ω- 群. (请读者自行验证.)

(4) 给定两个 Ω- 群 G_1, G_2, 称同态映射 ε: $G_1 \to G_2$ 为算子同态 (或 Ω- 同态), 如果

$$g^{\alpha\varepsilon} = g^{\varepsilon\alpha}, \qquad ,\forall \alpha \in \Omega, \quad g \in G_1.$$

仿此可定义算子同构 (或 Ω- 同构).

(5) 称 Ω- 群 G 为 *不可约的*, 如果 G 没有非平凡的正规 Ω- 子群.

容易验证, Ω- 群 G 的若干 Ω- 子群的交仍为 G 之 Ω- 子群; 而由 Ω- 子群生成的子群亦为 G 之 Ω- 子群.

对于任一给定之抽象群 G, 若取 $\Omega = \mathrm{Inn}(G)$ 使 G 为一 Ω- 群, 则 G 的 Ω- 子群即为通常的正规子群; 而若取 $\Omega = \mathrm{Aut}(G)$, 则 Ω- 子群为通常的特征子群; 若取 $\Omega = \mathrm{End}(G)$, 则 Ω- 子群为通常的全不变子群. 这样, 子群, 正规子群, 特征子群和全不变子群的概念都可统一在 Ω- 子群之中. (注意, 亦可取 $\Omega = \varnothing$, 这时 Ω- 群即为一般的抽象群, 而 Ω- 子群即为通常之子群.)

请读者自行验证在 I,§2 中讲过的群的同态及同构定理对于 Ω- 群也同样成立, 只要在其中把群, 子群, 同态, 同构相应换成 Ω- 群, Ω- 子群, Ω- 同态, Ω- 同构即可.

定义 1.2 设 G 是 Ω- 群. 称群列

$$G = G_0 \geq G_1 \geq G_2 \geq \ldots \geq G_r = 1 \tag{1.1}$$

为 G 的一个 *次正规 Ω- 群列*, 如果对于 $i = 1, 2, \ldots, r$, G_i 是 G 的 Ω- 子群, 且 $G_i \trianglelefteq G_{i-1}$.

我们又称 G 的次正规 Ω- 群列 (1.1) 为 G 的一个 *合成 Ω- 群列*, 如果对于 $i = 1, 2, \ldots, r$, G_i 是 G_{i-1} 的真子群, 并且 G_{i-1}/G_i 是不可约 Ω- 群.

若取 $\Omega = \varnothing$, 上述定义就给出了抽象群的次正规群列和合成群列的概念. 而若取 $\Omega = \mathrm{Inn}(G)$, 则称 Ω- 群 G 的次正规 Ω- 群列为抽象群 G 的 *正规群列* 或 *不变群列*, 而 Ω- 群 G 的合成 Ω- 群列为 抽象群 G 的 *主群列*, 这与本章开头时给出的主群列定义是一致的. 明显地, 对于 主群列, 每个主因子 G_{i-1}/G_i 都是特征单群. 自然我们还可取 $\Omega = \mathrm{Aut}(G)$ 来给出抽象群的特征群列的概念, 但目前研究得还不多, 这里不再叙述.

引理 1.3 (Zassenhaus) 设 $H_1 \trianglelefteq H \leq G$, $K_1 \trianglelefteq K \leq G$, 则有

$$H_1(H \cap K)/H_1(H \cap K_1) \cong K_1(H \cap K)/K_1(H_1 \cap K).$$

如果上式中出现的群均为 Ω- 群，则上述同构可为 Ω- 同构.

证 由 $K_1 \trianglelefteq K$, 有 $H \cap K_1 \trianglelefteq H \cap K$, 又有

$$H_1(H \cap K_1) \trianglelefteq H_1(H \cap K).$$

据第二同构定理，有

$$\begin{aligned} & H_1(H \cap K)/H_1(H \cap K_1) \\ = & \; H_1(H \cap K_1)(H \cap K)/H_1(H \cap K_1) \\ \cong & \; (H \cap K)/(H_1(H \cap K_1)) \cap (H \cap K). \end{aligned}$$

因 $H \cap K_1 \leq H \cap K$, 由 I,§1 末习题 15, 有

$$\begin{aligned} H_1(H \cap K_1) \cap (H \cap K) &= (H \cap K_1)(H_1 \cap (H \cap K)) \\ &= (H \cap K_1)(H_1 \cap K). \end{aligned}$$

代入上式得

$$H_1(H \cap K)/H_1(H \cap K_1) \cong (H \cap K)/(H \cap K_1)(H_1 \cap K).$$

同理

$$K_1(H \cap K)/K_1(H_1 \cap K) \cong H \cap K/(H_1 \cap K)(H \cap K_1),$$

故得结论.

又因同态定理及第一，第二同构定理对 Ω- 群都成立，故此引理对 Ω- 群亦成立. □

定理 1.4 (Schreier 加细定理) 设

$$G = G_0 \geq G_1 \geq \ldots \geq G_r = 1$$

和

$$G = H_0 \geq H_1 \geq \ldots \geq H_s = 1$$

是 Ω- 群 G 的两个次正规 Ω- 群列. 令

$$G_{ij} = G_i(G_{i-1} \cap H_j), \quad H_{ij} = H_j(G_i \cap H_{j-1}).$$

则在上述二群列中插入

$$G_{i-1} = G_{i0} \geq G_{i1} \geq \ldots \geq G_{is} = G_i, \quad i = 1, \ldots, r$$

和

$$H_{j-1} = H_{0j} \geq H_{1j} \geq \ldots \geq H_{rj} = H_j, \quad j = 1, \ldots, s,$$

得到的加细了的二群列仍为 G 的次正规 Ω- 群列, 并且

$$G_{i,j-1}/G_{ij} \cong H_{i-1,j}/H_{ij}, \quad \forall i, j.$$

简言之, 即: 任二次正规 Ω- 群列都有同构的加细.

证 显然, G_{ij} 和 H_{ij} 均为 G 的 Ω- 子群. 因为 $H_j \trianglelefteq H_{j-1}$, 有

$$G_{i-1} \cap H_j \trianglelefteq G_{i-1} \cap H_{j-1},$$

因此

$$G_{ij} = G_i(G_{i-1} \cap H_j) \trianglelefteq G_i(G_{i-1} \cap H_{j-1}) = G_{i,j-1}.$$

同理有 $H_{ij} \trianglelefteq H_{i-1,j}$. 于是上面作出的群列确为 G 的次正规 Ω- 群列. 现在据引理 1.3,

$$\begin{aligned} G_{i,j-1}/G_{ij} &= G_i(G_{i-1} \cap H_{j-1})/G_i(G_{i-1} \cap H_j) \\ &\cong H_j(G_{i-1} \cap H_{j-1})/H_j(G_i \cap H_{j-1}) \\ &\cong H_{i-1,j}/H_{ij}. \end{aligned}$$

定理得证. □

定理 1.5 (Jordan-Hölder) 设 G 是有限 Ω- 群

$$G = G_0 > G_1 > \ldots > G_r = 1$$

和

$$G = H_0 > H_1 > \ldots > H_s = 1$$

是 G 的两个合成 Ω- 群列. (注意, 有限群必存在合成群列 !) 则必有 $r = s$, 并且商群 G_i/G_{i+1} 和 H_j/H_{j+1} 适当编序后是同构的不可约 Ω- 群. 称它们为 G 的 Ω-合成因子.

证 和上定理相同, 作此二群列的加细, 即插入子群 G_{ij} 和 H_{ij}. 由于原群列已是合成 Ω- 群列. 故此加细实际上只是增添一些重复项而已. 据上定理, 加细后的二群列是同构的. 由此推知去掉重复项后仍然同构, 即得所需之结论. □

令 $\Omega = \varnothing$ 和 $\mathrm{Inn}(G)$, 由上定理即得到关于抽象群的合成群列和主群列的相应定理.

注 1.6 对于无限 Ω- 群 G, 合成 Ω- 群列的存在是有条件的. 这些条件即所谓无限群的有限性条件. 常见的有以下几种:

(1) 关于 Ω- 子群的 升链条件: 对于由 G 的 Ω- 子群组成的上升群列 (升链)

$$H_1 \leq H_2 \leq H_3 \leq \ldots,$$

总可找到正整数 k 使 $H_k = H_{k+1} = \ldots$.

(2) 关于 Ω- 子群的 降链条件: 对于由 G 的 Ω- 子群组成的下降群列 (降链)

$$G_1 \geq G_2 \geq G_3 \geq \ldots,$$

总可找到正整数 k 使 $G_k = G_{k+1} = \ldots$.

(3) 关于 Ω- 子群的 极大条件: 对于由 G 的 Ω- 子群组成的任一非空集合 $\mathcal{S}$, 总存在极大元素 $M \in \mathcal{S}$. 即 M 满足: 由 $H \in \mathcal{S}$ 和 $M \leq H$ 可推出 $H = M$.

(4) 关于 Ω- 子群的 极小条件: 对于由 G 的 Ω- 子群组成的任一非空集合 $\mathcal{S}$, 总存在极小元素 $M \in \mathcal{S}$. 即 M 满足: 由 $H \in \mathcal{S}$ 和 $M \geq H$ 可推出 $H = M$.

容易证明，升链条件 (1) 和极大条件 (3) 是等价的，降链条件 (2) 和极小条件 (4) 的等价的.

对于无限 Ω- 群 G 来说， G 存在合成 Ω- 群列的充要条件是 G 满足关于 Ω- 子群的两个链条件. (请读者自行证明.) 并且在这个前提之下， Jordan-Hölder 定理仍然成立，证明亦可不做改动.

有了 Jordan-Hölder 定理，我们可以给有限可解群一个新的刻画. 这在以后经常要用到.

定理 1.7 *设 G 为有限群. 则下述两条均为 G 可解之充要条件:*

(1) G 的合成因子皆为素数阶循环群;

(2) G 的主因子皆为素数幂阶的初等交换群.

证 (1) $\Leftarrow$: 设 G 有合成群列

$$G = G_0 > G_1 > \ldots > G_r = 1,$$

其中 G_{i-1}/G_i 是素数阶循环群， $i = 1, \ldots, r$. 这时可用归纳法证明对任意的 i 都有 $G^{(i)} \leq G_i$, 于是 $G^{(r)} = 1$, G 可解.

$\Rightarrow$: 由 G 可解，知每个合成因子 G_{i-1}/G_i 亦可解. 又由合成因子必为单群，故必为素数阶循环群.

(2) 由 (1) 及定理 I,2.17 立得. □

本节的以下部分将介绍次正规子群的概念，并证明它的两个最基本的性质.

定义 1.8 设 G 是群， $H \leq G$, 称 H 为 G 的 *次正规子群*, 并记作 $H \lhd \lhd G$, 如果 H 在 G 的某个次正规群列中出现.

显然， G 的正规子群都是次正规子群. 但由子群的正规性没有传递性，即由 $K \trianglelefteq H$ 和 $H \trianglelefteq G$ 一般不能推出 $K \trianglelefteq G$, G 的次正规子群不一定都是正规子群.

定理 1.9 *设 G 是群， $H \lhd \lhd G$, $K \lhd \lhd G$. 则 $H \cap K \lhd \lhd G$.*

证 因为 $H \lhd\lhd G$, $K \lhd\lhd G$, 可设 G 有次正规群列

$$G = H_0 \geq H_1 \geq \ldots \geq H_r = H \geq \ldots \geq 1$$

和

$$G = K_0 \geq K_1 \geq \ldots \geq K_s = K \geq \ldots \geq 1.$$

由 $H_i \trianglelefteq H_{i-1}$, $i = 1, \ldots, r$, 有 $K \cap H_i \trianglelefteq K \cap H_{i-1}$. 于是 K 有次正规群列

$$K = K \cap H_0 \geq K \cap H_1 \geq \ldots \geq K \cap H_r = K \cap H \geq \ldots \geq 1.$$

这得到 $K \cap H \lhd\lhd K$. 又, 显然次正规性具有传递性, 故由 $K \lhd\lhd G$ 和 $K \cap H \lhd\lhd K$ 可得 $K \cap H \lhd\lhd G$. □

定理 1.10 设 G 是有限群, $H \lhd\lhd G$, $K \lhd\lhd G$. 则 $\langle H, K\rangle \lhd\lhd G$.

为证明这个定理, 我们先引进下面的.

定义 1.11 设 G 是有限群, $H \lhd\lhd G$. 由 Schreier 加细定理, H 必在 G 的某个合成群列中出现. 又由 Jordan-Hölder 定理, H 在 G 的任一合成群列中出现的项数是一定的, 譬如说是第 l 项. (注意, G 本身算第 0 项.) 则我们记 $l = l_G(H)$, 称为 H关于 G 的合成长度.

因为 $1 \lhd\lhd G$, 1 关于 G 的合成长度 $l_G(H)$ 常简记作 l_G, 叫做 G 的 合成长度, 即群 G 的所有合成群列公共的长度. 如果 $H \lhd\lhd G$, 显然有 $l_G = l_G(H) + l_H$.

我们有下面的引理.

引理 1.12 设 G 是有限群, $H \lhd\lhd G$, $K \lhd\lhd G$, 且 $H < K$. 则 $l_G(H) > l_G(K)$.

证 为证明引理, 只须证 H 和 K 可以同时出现在 G 的某个次正规群列中, 从而也同时出现在 G 的某个合成群列中. 设

$$G = H_0 \geq H_1 \geq \ldots \geq H_r = H \geq \ldots \geq 1$$

和

$$G = K_0 \geq K_1 \geq \ldots \geq K_s = K \geq \ldots \geq 1$$

是 G 的分别包含 H 和 K 的两个次正规群列. 则

$$K = K \cap H_0 \geq K \cap H_1 \geq \ldots \geq K \cap H_r = H \geq \ldots \geq 1$$

是 K 的次正规群列, 而

$$\begin{aligned} G = K_0 \quad &\geq \quad K_1 \geq \ldots \geq K_s = K = K \cap H_0 \geq K \cap H_1 \\ &\geq \quad \ldots \geq K \cap H_r = H \geq \ldots \geq 1 \end{aligned}$$

就是满足条件的 G 的次正规群列. □

引理 1.13 设 G 是群, $H \trianglelefteq G$, $K \triangleleft\triangleleft G$. 则 $\langle H, K\rangle = HK \triangleleft\triangleleft G$.

证 首先, 若 $A \trianglelefteq B \leq G$, $H \trianglelefteq G$, 则 $AH \trianglelefteq BH$. 这是因为对任意的 $b \in B$, $h \in H$, 有

$$(AH)^b = A^bH^b = AH, \quad (AH)^h = A^hH \supseteq HAH = AH.$$

现在设

$$G = K_0 \geq K_1 \geq \ldots \geq K_s = K \geq \ldots \geq 1$$

是 G 的次正规群列. 因为 $K_i \trianglelefteq K_{i-1}$, $i = 1, \ldots, s$, 故

$$G = K_0H \geq K_1H \geq \ldots \geq K_sH = HK \geq H = 1$$

也是 G 的次正规群列. 引理得证. □

定理 1.10 的证明: 设 $l_G(H) = r$, $l_G(K) = s$. 并设

$$G = H_0 > H_1 > \ldots > H_r = H > \ldots > 1$$

和

$$G = K_0 > K_1 > \ldots > K_s = K > \ldots > 1$$

是 G 的两个分别包含 H 和 K 的合成群列. 由对称性, 不妨设 $r \geq s$. 用对 $r+s$ 的归纳法. 当 $r+s \leq 2$ 时结论是明显的. 由归纳假设, 可令 $M = \langle H_r, K_{s-1}\rangle \lhd \lhd G$. 如果 M 是 G 的真子群, 则由引理 1.12, $l_M(H) < r$, $l_M(K) < s$, 再由归纳假设, 有 $\langle H, K\rangle \lhd \lhd M$, 自然也有 $\langle H, K\rangle \lhd \lhd G$. 故可设 $M = G$. 假若 $K \trianglelefteq G$, 由引理 1.13 可得 $\langle H, K\rangle \lhd \lhd G$. 故又可设 $K \ntrianglelefteq G$, 这时必有 $h \in H$ 使 $K^h \neq K$. 考虑 G 的次正规子群

$$G = K_0 > K_1 > \ldots > K_{s-1} > K_s = K > \ldots > 1$$

和

$$G = K_0 > K_1^h = K_1 > \ldots > K_{s-1}^h > K_s^h = K^h > \ldots > 1,$$

应用归纳假设于 K_1, 注意到 $r \geq s$, 可得 $\langle K, K^h\rangle \lhd \lhd K_1$, 自然也有 $\langle K, K^h\rangle \lhd \lhd G$. 又因 $\langle K, K^h\rangle > K$, 由引理 1.12, 有 $l_G(\langle K, K^h\rangle) < l_G(K) = s$. 于是归纳假设又给出 $\langle H, K, K^h\rangle \lhd \lhd G$. 而 $\langle H, K, K^h\rangle = \langle H, K\rangle$, 定理得证. □

注 1.14 (1) 定理 1.10 不仅对有限群成立, 而且对每个存在合成群列的群都成立. 证明可不加改动.

(2) 但一般来说, 定理 1.10 对无限群不真. Zassenhaus 举出一个反例, 可见他写的 “The Theory of Groups” 1958 年英文版中附录 D 的第 23 题.

关于有限群的次正规子群还有很多有趣的性质, 可参看研究题 4.

§2. 直积分解

本节的主要目的是对有限群来证明 Krull-Schmidt 直积分解唯一性定理 (定理 2.15). 首先, 我们继续讲述 Ω- 群的理论.

本节中恒假定 G 是 Ω- 群, 并仍以 End(G) 表示 G 的全体自同态组成的集合.

定义 2.1 称 $\mu\in \mathrm{End}(G)$ 为 G 的**正规自同态**, 如果 μ 与 G 的所有内自同构可交换.

命题 2.2 设 μ 是群 G 的正规自同态, 则 $G^\mu \trianglelefteq G$, 并且对任意的 $g\in G$ 有 $g^\mu g^{-1}\in C_G(G^\mu)$.

证　对任意的 $g,h\in G$, 我们以 $\sigma(g)$ 表由 g 诱导出的 G 的内自同构, 由 μ 是正规自同态, 便有

$$g^{-1}h^\mu g = h^{\mu\sigma(g)} = h^{\sigma(g)\mu}\in G^\mu,$$

由此即得 $G^\mu \trianglelefteq G$. 又因

$$\begin{aligned} g^\mu g^{-1}\cdot h^\mu (g^\mu g^{-1})^{-1} &= g^\mu h^{\mu\sigma(g)}(g^{-1})^\mu = g^\mu h^{\sigma(g)\mu}(g^{-1})^\mu \\ &= (gh^{\sigma(g)}g^{-1})^\mu = h^\mu, \end{aligned}$$

并由 h 的任意性得 $g^\mu g^{-1}\in C_G(G^\mu)$. □

定义 2.3 称 $\mu\in \mathrm{End}(G)$ 为 Ω- 群 G 的 Ω- **自同态**, 如果 μ 与 Ω 中每个自同态可交换.

G 的全体 Ω- 自同态的集合记作 $\mathrm{End}_\Omega(G)$.

我们以 1 记 G 到自身的恒等映射, 而以 0 记把 G 的每个元素映到单位元素上的自同态. 显然, 1 和 0 都是 G 的 Ω- 自同态.

命题 2.4 设 $\mu\in \mathrm{End}_\Omega(G)$, 则 G^μ 和 $\mathrm{Ker}\,\mu$ 都是 G 的 Ω- 子群. 又若 μ 是正规 Ω- 自同构, 则 G^μ 和 $\mathrm{Ker}\,\mu$ 都是 G 的正规 Ω- 子群.

证　对于任意的 $\alpha\in\Omega$, 因为

$$(G^\mu)^\alpha = G^{\mu\alpha} = G^{\alpha\mu}\le G^\mu,$$

故 G^μ 是 G 的 Ω- 子群. 又对任意的 $x\in \mathrm{Ker}\,\mu$, 有 $x^\mu=1$. 于是 $(x^\alpha)^\mu = x^{\alpha\mu} = x^{\mu\alpha} = 1^\alpha = 1$, 即 $x^\alpha\in \mathrm{Ker}\,\mu$. 这说明 $\mathrm{Ker}\,\mu$ 是 G 的 Ω- 子群. $\mathrm{Ker}\,\mu$ 作为 μ 的核, 当然是 G 的正规子群. 最后, 若 μ 是正规自同态, 由命题 2.2, $G^\mu \trianglelefteq G$. 定理得证. □

关于正规 Ω- 自同态最重要的结果是下面的两个定理.

定理 2.5 (Schur) 设 G 是不可约 Ω- 群，μ 是 G 的正规 Ω- 自同态．若 $\mu\neq 0$, 则 μ 是 G 的 Ω- 自同构，并且 μ^{-1} 亦然．

证 因为 μ 是 G 的正规 Ω- 自同态，由命题 2.4, G^{μ} 是 G 的正规 Ω- 子群．再由 G 的不可约性及 $\mu\neq 0$ 得 $G^{\mu}=G$. 另一方面， $\mathrm{Ker}\,\mu$ 也是 G 的正规 Ω- 子群，再用 $\mu\neq 0$, 得 $\mathrm{Ker}\,\mu\neq G$, 于是 $\mathrm{Ker}\,\mu=1$. 这样 μ 是 G 到自身上的一一映射，即 μ 是 G 的自同构．

因为 μ 是 G 的自同构，当然 μ^{-1} 亦然．为完成证明，还要证 μ^{-1} 是正规 Ω- 自同态，即 μ^{-1} 与每个 $\alpha\in\Omega$ 以及每个内自同构 $\sigma(g)$ 可交换．这只须在等式

$$\mu\alpha=\alpha\mu$$

及

$$\mu\sigma(g)=\sigma(g)\mu$$

的两端同时左乘并右乘 μ^{-1} 即可得到

$$\alpha\mu^{-1}=\mu^{-1}\alpha$$

及

$$\sigma(g)\mu^{-1}=\mu^{-1}\sigma(g),$$

定理得证． □

定理 2.6 (Fitting) 设 G 是 Ω- 群，满足关于正规 Ω- 子群的两个链条件．如果 μ 是正规 Ω- 自同态，则对充分大的正整数 k 有

$$G=G^{\mu^k}\times\mathrm{Ker}\,\mu^k.$$

证 容易看出，对任意正整数 m, μ^m 也是 G 的正规 Ω- 自同态．于是可考虑的正规 Ω- 群列

$$G\geq G^{\mu}\geq G^{\mu^2}\geq\cdots,$$

根据降链条件，存在正整数 m 使

$$G^{\mu^m} = G^{\mu^{m+1}} = \cdots.$$

再考虑正规 Ω- 群列

$$1 \le \text{Ker } \mu \le \text{Ker } \mu^2 \le \cdots,$$

根据升链条件，存在正整数 n 使

$$\text{Ker } \mu^n = \text{Ker } \mu^{n+1} = \cdots.$$

取 $k = \max(m, n)$, 则有

$$\text{Ker } \mu^k = \text{Ker } \mu^{k+1} = \cdots$$

和

$$G^{\mu^k} = G^{\mu^{k+1}} = \cdots.$$

我们证明这时必有 $G = G^{\mu^k} \times \text{Ker } \mu^k$.

首先，G^{μ^k} 和 Ker μ^k 都是 G 的正规 Ω- 子群. 为完成证明还只须证 $G^{\mu^k} \cap \text{Ker } \mu^k = 1$ 和 $G = G^{\mu^k} \cdot \text{Ker } \mu^k$. 设 $g \in G^{\mu^k} \cap \text{Ker } \mu^k$, 则有 $g^{\mu^k} = 1$, 并且存在 $h \in G$ 使 $h^{\mu^k} = g$. 于是 $h^{\mu^{2k}} = 1$. 这样 $h \in \text{Ker } \mu^{2k} = \text{Ker } \mu^k$, 由此又得 $h^{\mu^k} = 1$, 即 $g = 1$. 这证明了 $G^{\mu^k} \cap \text{Ker } \mu^k = 1$. 再设 $g \in G$, 则 $g^{\mu^k} \in G^{\mu^k} = G^{\mu^{2k}}$. 于是存在 $h \in G$ 使 $g^{\mu^k} = h^{\mu^{2k}} = (h^{\mu^k})^{\mu^k}$. 这时有 $g = (gh^{-\mu^k})^{\mu^k} \in \text{Ker } \mu^k$. 这证明了 $G = G^{\mu^k} \cdot \text{Ker } \mu^k$, 定理得证. □

定义 2.7 称 Ω- 群 G 为**不可分解的**, 如果 G 不能表成两个非平凡 Ω- 子群的直积.

推论 2.8 设 G 是不可分解 Ω- 群，满足关于正规 Ω- 子群的两个链条件. 若 μ 是 G 的正规 Ω- 自同态，则或者 μ 为自同构，或者 $\mu^k = 0$, 对某正整数 k 成立.

证 由定理 2.6, 对某正整数 k 有

$$G = G^{\mu^k} \times \text{Ker } \mu^k.$$

因为 G 不可分解，或者 $G^{\mu^k}=1$, 或者 $\mathrm{Ker}\ \mu^k=1$. 这就推出或者 $\mu^k=0$, 或者 $\mathrm{Ker}\ \mu=1$, 如果出现后者又有 $G^{\mu^k}=G$, 于是有 $G^\mu=G$, 即 μ 是自同构. □

定义 2.9 设 G 为群， $\mu,\nu\in\mathrm{End}(G)$. 称 μ,ν 为**可加的**, 并记 $\mu+\nu=\varepsilon$, 如果如下定义的映射 ε 仍为 G 之自同态:

$$\varepsilon: g\mapsto g^\mu g^\nu,\ \forall g\in G.$$

命题 2.10 设 $\mu,\nu\in\mathrm{End}(G)$. 则 μ,ν 可加的充要条件为 G^μ 与 G^ν 元素间可交换.

证

$$\begin{aligned}\mu,\nu\text{可加}\quad&\Longleftrightarrow\quad \varepsilon=\mu+\nu\ \text{是}\ G\ \text{的自同态}\\&\Longleftrightarrow\quad (gh)^{\mu+\nu}=g^{\mu+\nu}h^{\mu+\nu},\ \forall g,h\in G\\&\Longleftrightarrow\quad (gh)^\mu(gh)^\nu=g^\mu g^\nu h^\mu h^\nu,\ \forall g,h\in G\\&\Longleftrightarrow\quad h^\mu g^\nu=g^\nu h^\mu,\ \forall g,h\in G.\end{aligned}$$

□

容易验证，若 G 为 Ω- 群， $\mu,\nu\in\mathrm{End}_\Omega(G)$, 且 μ,ν 可加，则 $\mu+\nu\in\mathrm{End}_\Omega(G)$. 又若 μ,ν 为正规 Ω- 自同态，则 $\mu+\nu$ 亦为正规 Ω- 自同态.

命题 2.11 设 G 是不可分解的 Ω- 群，满足关于正规 Ω- 子群的两个链条件. 若 μ,ν 是 G 的可加的正规 Ω- 自同态，且 $\varepsilon=\mu+\nu$ 是 G 的自同构，则 μ,ν 中至少有一个是 G 的自同构.

证 令 $\mu'=\mu\varepsilon^{-1},\nu'=\nu\varepsilon^{-1}$. 因为 μ,ν 可加，由命题 2.10 有

$$h^\mu g^\nu=g^\nu h^\mu,\ \forall g,h\in G.$$

用 ε^{-1} 作用于上式两端，得到

$$h^{\mu'}g^{\nu'}=g^{\nu'}h^{\mu'},\ \forall g,h\in G,$$

即 μ',ν' 亦可加. 并且容易验证 μ',ν' 仍为 G 的正规 Ω- 自同态, 且满足 $\mu'+\nu'=1$. 于是有

$$\mu'\nu'=\mu'(1-\mu')=(1-\mu')\mu'=\nu'\mu',$$

其中映射 $1-\mu'$ 规定为

$$g^{1-\mu'}=g(g^{-1})^{\mu'}=g(g^{\mu'})^{-1},\ \forall g\in G.$$

假定 μ',ν' 都不是 G 的自同构, 由推论 2.8, 对充分大的正整数 k 有 $\mu'^k=0$, $\nu'^k=0$. 于是

$$1=(\mu'+\nu')^{2k}=\sum_{j=0}^{2k}\binom{2k}{j}\mu'^{2k-j}\nu'^j=0,$$

矛盾. 故 μ',ν' 中至少有一个, 譬如 μ' 是自同构, 于是 $\mu=\mu'\varepsilon$ 也是 G 的自同构. □

应用归纳法易得到

命题 2.11′　设 G 是不可分解 Ω- 群, 满足关于正规 Ω- 子群的两个链条件. 若 $\mu_1,\mu_2,\cdots,\mu_s$ 是 G 的两两可加的正规 Ω- 自同态, 且 $\varepsilon=\mu_1+\mu_2+\cdots+\mu_s$ 是 G 的自同构, 则存在一个 μ_i, $1\le i\le s$, 是 G 的自同构. (证明从略.)

下面考虑有限 Ω- 群的直积分解. 我们先证明

引理 2.12 设 G 是 Ω- 群, $G_1,\cdots,G_n$ 是 G 的 Ω- 子群, 并且 $G=G_1\times\cdots\times G_n$. 对于每个 $i=1,2,\cdots,n$, 如下定义 G 的射影 π_i: 若 $g=g_1\cdots g_n$, 其中 $g_1\in G_1,\cdots,g_n\in G_n$, 则规定 $g^{\pi_i}=g_i$. 我们有 $\pi_i\in\mathrm{End}_\Omega(G)$, $i=1,\cdots,n$, 是 G 的两两可加的正规 Ω- 自同态, 并且成立

$$\pi_1+\cdots+\pi_n=1;$$
$$\pi_i^2=\pi_i, i=1,\cdots,n;$$
$$\pi_i\pi_j=0, i,j=1,\cdots,n,\ 且 i\neq j.$$

证 设 $g = g_1 \cdots g_n, h = h_1 \cdots h_n$, 其中 $g_i, h_i \in G_i$, $i = 1, \cdots, n$. 则

$$gh = g_1 \cdots g_n h_1 \cdots h_n = g_1 h_1 \cdots g_n h_n.$$

所以

$$(gh)^{\pi_i} = g_i h_i = g^{\pi_i} h^{\pi_i},$$

即 π_i 是自同态. 又设 $\alpha \in \Omega$, 因 $G_i^\alpha \le G_i$, 有

$$G^{\alpha\pi_i} = (G^\alpha)^{\pi_i} = (G_1^\alpha \cdots G_n^\alpha)^{\pi_i} = G_i^\alpha = G^{\pi_i \alpha},$$

故 $\pi_i \in \mathrm{End}_\Omega(G)$.

又因对 $i \neq j$, $G^{\pi_i} = G_i$ 和 $G^{\pi_j} = G_j$ 元素之间可交换, 由命题 2.10 得 π_i, π_j 可加.

最后, 等式 $\pi_1 + \cdots + \pi_n = 1$, $\pi_i^2 = \pi_i$, $\pi_i \pi_j = 0 (i \neq j)$ 属直接验证, 显然成立. 引理得证. □

因为在直积分解式中出现的子群皆为正规子群, 故可假定 Ω 包含 G 的全部内自同构. 这样 Ω- 子群就都是正规子群, Ω- 自同态也都是正规自同态. 这可使叙述得到简化. 因此在本节的以下部分, 我们恒作这样的假定.

引理 2.13 *设 G, H 是 Ω- 群. 如果 π 是 G 到 H 的 Ω- 同态, μ 是 H 到 G 的 Ω- 同态, 且 $\pi\mu$ 是 G 的自同构, 则 $H = G^\pi \times \mathrm{Ker}\,\mu$.*

证 首先, G^π 和 $\mathrm{Ker}\,\mu$ 都是 H 的 Ω- 子群; 且因为我们假定 Ω 包含 H 的全体内自同构, 它们也都是 H 的正规子群. 因此为完成证明只须证 $G^\pi \cap \mathrm{Ker}\,\mu = 1$ 和 $H = G^\pi \cdot \mathrm{Ker}\,\mu$.

设 $h \in G^\pi \cap \mathrm{Ker}\,\mu$. 则对某个 $g \in G$, 有 $h = g^\pi$, 同时又有 $h^\mu = g^{\pi\mu} = 1$. 因为 $\pi\mu$ 是 G 的自同构, 得 $g = 1$, 于是 $h = 1$. 这证明了 $G^\pi \cap \mathrm{Ker}\,\mu = 1$.

又对任一 $h \in H$, 有 $h^\mu \in G$. 因 $\pi\mu$ 是 G 的自同构, 存在 $g \in G$ 使 $g^{\pi\mu} = h^\mu$, 故 $(hg^{-\pi})^\mu = 1$, 即 $hg^{-\pi} \in \mathrm{Ker}\,\mu$. 于是由

$$h = hg^{-\pi} \cdot g^\pi \in \mathrm{Ker}\,\mu \cdot G^\pi,$$

得 $H=G^{\pi}\cdot\mathrm{Ker}\,\mu$. 至此已得 $H=G^{\pi}\times\mathrm{Ker}\,\mu$. □

定理 2.14 (Krull-Schmidt) 设 G 是有限 Ω- 群，则 G 可分解为有限个不可分解的 Ω- 子群的直积

$$G=G_1\times\cdots\times G_r.$$

又若 $G=H_1\times\cdots\times H_s$ 也是 G 的不可分解 Ω- 子群的直积分解式，则有 $r=s$, 并且对诸 H_i 适当编序后有 Ω- 同构 $G_i\cong H_i$, $i=1,\cdots,r$.

证 因 G 是有限群，可分解性是显然的. 故只须证唯一性. 对 r 用归纳法. 当 $r=1$, 这时 G 不可分解，结论显然成立. 下面设 $r>1$. 假定 $\pi_1,\cdots,\pi_r$ 和 $\mu_1,\cdots,\mu_s$ 是对应于二分解式的射影. 有

$$1=\pi_1+\cdots+\pi_r=\mu_1+\cdots+\mu_s;$$

$$\pi_i^2=\pi,\ \mu_i^2=\mu;\ \pi_i\pi_j=\mu_i\mu_j=0,\ i\neq j.$$

由此推出

$$\pi_1=(\mu_1+\cdots+\mu_s)\pi_1=\mu_1\pi_1+\cdots+\mu_s\pi_1.$$

把上述映射限制在 G_1 上，因 π_1 是 G_1 的自同构，由命题 2.11, $\mu_1\pi_1,\cdots,\mu_s\pi_1$ 中至少有一个是 G_1 的自同构. 不妨设 $\mu_1\pi_1$ 是 G_1 的自同构. 考虑映射

$$G_1\xrightarrow{\mu_1}H_1\xrightarrow{\pi_1}G_1,$$

由引理 2.13, $H_1=G_1^{\mu_1}\times\mathrm{Ker}\,\pi_1$. 又因 μ_1 必为单射，π_1 为满射，有 $G_1^{\mu_1}\neq 1$, $\mathrm{Ker}\,\pi_1\neq H_1$. 据 H_1 的不可分解性，得 $G_1^{\mu_1}=H_1$, $\mathrm{Ker}\,\pi_1=1$. 这样 μ_1 是 G_1 到 H_1 的 Ω- 同构，π_1 是 H_1 到 G_1 的 Ω- 同构.

现在我们再证明 $\overline{G}=H_1(G_2\times\cdots\times G_r)$ 也是直积，这只要证单位元素 1 的表法唯一. 令

$$1=h_1g_2\cdots g_r,\ h_1\in H_1,g_2\in G_2,\cdots,g_r\in G_r,$$

以 π_1 作用在上式两端得 $h_1^{\pi_1}=1$. 因 π_1 是 H_1 到 G_1 的同构，故得 $h_1=1$. 于是又有 $g_2\cdots g_r=1$, 从而得到 $g_2=1,\cdots,g_r=1$. 这样

$$\overline{G}=H_1\times G_2\times\cdots\times G_r.$$

因为 $\overline{G}\leq G$, 比较阶即得 $G=H_1\times G_2\times\cdots\times G_r$. 于是

$$G/H_1\cong G_2\times\cdots\times G_r.$$

又因 $G=H_1\times H_2\times\cdots\times H_s$, 有

$$G/H_1\cong H_2\times\cdots\times H_s.$$

所以

$$G_2\times\cdots\times G_r\cong H_2\times\cdots\times H_s.$$

设 α 是上述同构的一个同构映射，则有

$$G_2^\alpha\times\cdots\times G_r^\alpha=H_2\times\cdots\times H_s.$$

于是由归纳假设即得 $r=s$, 并对诸 H_i 适当编序后有 $G_2^\alpha\cong H_2,\cdots,G_r^\alpha\cong H_r$. 而因 $G_i^\alpha\cong G_i$, 故得 $G_i\cong H_i$, $i=2,\cdots,r$. 定理证毕. □

注 2.15 定理 2.14 对关于正规 Ω- 子群满足两个链条件的无限 Ω- 群亦成立，证明只有两处需要改动：一处是需用两个链条件推出 G 可分解为有限多个不可分解的 Ω- 子群的直积，请读者自行证明. 另一处是要证 $\overline{G}=G$(比较阶的方法对无限群已行不通), 这可如下进行：令

$$\rho=\pi_1\mu_1+\pi_2+\cdots+\pi_r,$$

则 ρ 是 G 到 $\overline{G}$ 的映射. 由 $H_1\times G_2\times\cdots\times G_r$ 是直积可推出 $\pi_1\mu_1,\pi_2,\cdots,\pi_r$ 两两可加，于是 $\rho\in\mathrm{End}_\Omega(G)$. 并且易证 ρ 是单同态，于是 ρ 是 G 到 $\overline{G}$ 上的同构. 考虑

$$G\geq G^\rho\geq G^{\rho^2}\geq\cdots,$$

由降链条件存在 k 使 $G^{\rho^k}=G^{\rho^{k+1}}=\cdots$, 故对 $g\in G$, 可找到 $\bar{g}\in G$ 使 $g^{\rho^k}=\bar{g}^{\rho^{k+1}}$. 从而推出 $(g\bar{g}^{-\rho})^{\rho^k}=1$. 由 ρ 是单射， $g\bar{g}^{-\rho}=1$, 这样就得到 $g=\bar{g}^{\rho}$, 故 $G^{\rho}=G$, 于是 ρ 又是满射，即 $G=\overline{G}$.

§3. 群的扩张理论

由 Jordan-Hölder 定理，决定有限群构造的问题可分为两个问题：第一，决定所有的有限单群，它们是构造有限群的材料；第二，已知有限群的诸合成因子，来构造该群. 这两个问题都很困难. 第一个问题多年来一直是有限群论工作者主攻的课题，几年前才获得解决. 而对第二个问题的研究虽然已得到不少有意义的结果，但离彻底解决还为时尚远. 本节要讲述的 Schreier 群扩张理论是从原则上给出了由两个群构造一个大群的方法，但具体实现则十分困难.

定义 3.1 称群 G 为*群 N 被群 F 的扩张*, 如果 N 是 G 的正规子群，并且 $G/N\cong F$.

下面的叙述十分冗长的定理就是 Schreier 对群扩张问题的回答. 它实质上是把寻找已知群 N 被 F 的扩张的问题转化为寻找由 N,F 可以确定的满足一定条件的*扩张函数*的问题.

定理 3.2 (Schreier) *给定抽象群 N 和 F.*

(1) 设群 G 是 N 被 F 的一个扩张，并取定 σ 为 F 到 G/N 上的一个同构映射. 对于 $x\in F$, 令 $\bar{x}$ 是 x^{σ} 作为 N 的左陪集中的任一指定的代表元，但规定取 $\bar{1}=1$.[1] *这时得到 G 关于 N 的陪集分解*

$$G=N\cup\bar{x}N\cup\bar{y}N\cup\cdots\cup\bar{z}N,\ x,y,\cdots,z\in F. \tag{3.1}$$

因为 $\bar{x}\cdot\bar{y}\in(xy)^{\sigma}=\overline{xy}N$, 故可令

$$\bar{x}\cdot\bar{y}=\overline{xy}f(x,y),\ \text{其中} f(x,y)\in N.$$

[1]为符号简便计，我们对 F 中的 1 和 N 中的 1 不加区别，并且对 N 中元素 $f(x,y)$ 和由它诱导出的 N 的内自同构亦不加区别. 应注意区分.

这确定了一个二元函数 $f: F\times F\to N$. 又因 $N\trianglelefteq G$, 对任意的 $x\in F$, 映射

$$\alpha(x): a\mapsto \bar{x}^{-1}a\bar{x},\ a\in N$$

是 N 的自同构. 这又确定了一个单值映射 $\alpha: F\to \mathrm{Aut}(N)$. 这两个函数 f 和 α 叫做由扩张 G 及陪集代表系 $\{1,\bar{x},\bar{y},\cdots,\bar{z}\}$ 得到的扩张函数, 它们满足下列关系: 对任意的 $x,y,z\in F$ 有

$$\left.\begin{array}{l} f(xy,z)f(x,y)^{\alpha(z)}=f(x,yz)f(y,z),\\ f(1,1)=1,\\ \alpha(x)\alpha(y)=\alpha(xy)f(x,y). \end{array}\right\} \tag{3.2}$$

(2) 设给定了满足 (3.2) 式的函数 $f: F\times F\to N$ 和 $\alpha: F\to \mathrm{Aut}(N)$. 考虑下列符号组成的集合

$$G=\{\bar{x}a \mid x\in F, a\in N\}.$$

规定 G 中的乘法为

$$\bar{x}a\cdot\bar{y}b=\overline{xy}f(x,y)a^{\alpha(y)}b. \tag{3.3}$$

则 G 对此乘法组成一群. 若把 $\bar{1}a$ 和 a 等同看待, N 可看成是 G 的子群, 它是正规子群, 并且 $G/N\cong F$. 于是, G 是 N 被 F 的扩张. 这样得到的群 G 叫做由 N,F 以及函数 f,α 得到的扩张, 记作 $G=\mathrm{Ext}(N,F;f,\alpha)$. 这时若再把 $\bar{x}1$ 和 $\bar{x}$ 等同看待, 则 G 有形如 (3.1) 式的陪集分解, 且 $\{1,\bar{x},\bar{y},\cdots,\bar{z}\}$ 是其陪集代表系. 由此陪集代表系按 (1) 中的方法得到的扩张函数即为给定的函数 f 和 α.

证 (1) 由

$$\begin{aligned} (\bar{x}\bar{y})\bar{z} &= \overline{xy}f(x,y)\bar{z}=\overline{xy}\ \bar{z}(\bar{z}^{-1}f(x,y)\bar{z})\\ &= \overline{xyz}f(xy,z)f(x,y)^{\alpha(z)},\\ \bar{x}(\bar{y}\bar{z}) &= \bar{x}\ \overline{yz}f(y,z)=\overline{xyz}f(x,yz)f(y,z), \end{aligned}$$

及

$$(\bar{x}\bar{y})\bar{z}=\bar{x}(\bar{y}\bar{z}),$$

得

$$f(xy,z)f(x,y)^{\alpha(z)}=f(x,yz)f(y,z).$$

又因取 $\bar{1}=1$, 由 $\bar{1}\bar{1}=\bar{1}f(1,1)$ 得 $f(1,1)=1$.

对于 $a\in N$, 由

$$\begin{aligned} a^{\alpha(x)\alpha(y)} &= \bar{y}^{-1}\bar{x}^{-1}a\bar{x}\bar{y} \\ &= f(x,y)^{-1}\overline{xy}^{-1}a\overline{xy}f(x,y) \\ &= a^{\alpha(xy)f(x,y)}, \end{aligned}$$

得

$$\alpha(x)\alpha(y)=\alpha(xy)f(x,y).$$

于是 (3.2) 式成立.

(2) 显然 (3.3) 式规定了集合 G 中的一个二元运算. 为证明 G 是群, 需逐条检验群的公理. 首先, 由 (3.3) 式有

$$\begin{aligned} (\bar{x}a\bar{y}b)\bar{z}c &= \overline{xy}f(x,y)a^{\alpha(y)}b\bar{z}c \\ &= \overline{xyz}f(xy,z)(f(x,y)a^{\alpha(y)}b)^{\alpha(z)}c \\ &= \overline{xyz}f(xy,z)f(x,y)^{\alpha(z)}a^{\alpha(y)\alpha(z)}b^{\alpha(z)}c, \\ \bar{x}a(\bar{y}b\bar{z}c) &= \bar{x}a\overline{yz}f(y,z)b^{\alpha(z)}c \\ &= \overline{xyz}f(x,yz)a^{\alpha(yz)}f(y,z)b^{\alpha(z)}c \\ &= \overline{xyz}f(x,yz)f(y,z)a^{\alpha(yz)f(y,z)}b^{\alpha(z)}c, \end{aligned}$$

再由 (3.2) 式得 $(\bar{x}a\bar{y}b)\bar{z}c=\bar{x}a(\bar{y}b\bar{z}c)$, 于是成立结合律.

又, 在 (3.2) 式中令 $x=y=1$, 得

$$f(1,z)f(1,1)^{\alpha(z)}=f(1,z)f(1,z),$$

$$\alpha(1)\alpha(1)=\alpha(1)f(1,1),$$

注意到 $f(1,1)=1$, 于是有

$$f(1,z)=1,\quad \alpha(1)=1. \tag{3.4}$$

应用 (3.4) 式，由计算得

$$\bar{1}1\cdot\bar{x}a=\bar{x}f(1,x)1^{\alpha(x)}a=\bar{x}\cdot 1\cdot 1\cdot a=\bar{x}a,$$

推知 $\bar{1}1$ 是 G 的左单位元. 又对任意的 $\bar{x}a\in G$,

$$\begin{aligned}&\overline{x^{-1}}(f(x^{-1},x)^{-1}a^{-1})^{\alpha(x)^{-1}}\cdot\bar{x}a\\=\ &\overline{x^{-1}x}f(x^{-1},x)(f(x^{-1},x)^{-1}a^{-1})^{\alpha(x)^{-1}\alpha(x)}a\\=\ &\bar{1}f(x^{-1},x)f(x^{-1},x)^{-1}a^{-1}a=\bar{1}1,\end{aligned}$$

于是 $\bar{x}a$ 有左逆元 $\overline{x^{-1}}(f(x^{-1},x)^{-1}a^{-1})^{\alpha(x)^{-1}}$. 至此， G 对乘法 (3.3) 已成为一群.

再由 (3.4) 式计算得

$$\bar{1}a\cdot\bar{1}b=\bar{1}f(1,1)a^{\alpha(1)}b=\bar{1}ab,$$

故映射 $a\mapsto\bar{1}a$ 是 N 到 $\{\bar{1}a\mid a\in N\}\le G$ 的同构. 我们若把 a 和 $\bar{1}a$ 等同看待，就有 $N\le G$. 为证明 $N\trianglelefteq G$, 我们计算

$$(\bar{x}b)^{-1}\bar{1}a(\bar{x}b).$$

据 (3.3) 式得

$$\begin{aligned}(\bar{x}b)^{-1}\bar{1}a(\bar{x}b)&=\overline{x^{-1}}(f(x^{-1},x)^{-1}b^{-1})^{\alpha(x)^{-1}}\bar{x}f(1,x)a^{\alpha(x)}b\\&=\overline{x^{-1}}(f(x^{-1},x)^{-1}b^{-1})^{\alpha(x)^{-1}}\bar{x}a^{\alpha(x)}b\\&=\bar{1}f(x^{-1},x)(f(x^{-1},x)^{-1}b^{-1})^{\alpha(x)^{-1}\alpha(x)}a^{\alpha(x)}b\\&=\bar{1}f(x^{-1},x)f(x^{-1},x)^{-1}b^{-1}a^{\alpha(x)}b\\&=\bar{1}b^{-1}a^{\alpha(x)}b\in N,\end{aligned}$$

故 $N\trianglelefteq G$. 最后因

$$\bar{x}1\cdot\bar{1}a=\bar{x}1^{\alpha(1)}a=\bar{x}a,$$

故若把 $\bar{x}$ 和 $\bar{x}1$ 等同起来，则 $\bar{x}a$ 可看成是 $\bar{x}$ 和 a 的乘积，于是 G 有和 (3.1) 式相同的陪集分解式. 明显的，映射 $x \mapsto \bar{x}N$ 是 F 到 G/N 的同构. 这时因为

$$\begin{aligned}
\bar{x}\cdot\bar{y} &= \bar{x}1\cdot\bar{y}1 = \overline{xy}f(x,y)1^{\alpha(y)}1 = \overline{xy}f(x,y),\\
\bar{x}^{-1}a\bar{x} &= \overline{x^{-1}}(f(x^{-1},x)^{-1})^{\alpha(x)^{-1}}a\bar{x}1\\
&= \bar{1}f(x^{-1},x)(f(x^{-1},x)^{-1})^{\alpha(x)^{-1}\alpha(x)}a^{\alpha(x)}\cdot 1\\
&= a^{\alpha(x)},
\end{aligned}$$

故由陪集代表系 $\{1,\bar{x},\bar{y},\cdots,\bar{z}\}$ 按 (1) 中的方法所得到的扩张函数即预先给定的 f 和 α. 定理证毕. □

现在我们停下来看看这个定理对群扩张问题解决的程度. 它回答了哪些问题，又对哪些问题没有作出回答.

首先，对于任意给定的群 N 和 F, N 被 F 的扩张总是存在的. 这是因为函数 $f(x,y)=1$, $\alpha(x)=1$ 总满足 (3.2) 式，而这时对应的扩张 $G=N\times F$, 是 N 和 F 的直积.

既然存在性不成问题，下面的问题就是要问怎样把它们都找出来？并且从同构的意义上来说，究竟有多少个扩张？定理 3.2 对第一个问题的回答是，只要能把满足 (3.2) 式的所有可能的函数对 f,α 都找出来，所有的扩张也就无一遗漏地都找了出来. 但显然找满足条件的扩张函数的问题是十分困难而繁复的. 定理对第二个问题完全没作回答. 明显地，不同的扩张函数是能给出同构的扩张的. 但寻找给出同构扩张的两对扩张函数应满足的条件则是十分困难的问题，这就是所谓"同构问题"，目前人们对它基本上来说还束手无策. (当然，也解决了一些极简单的情形，如循环群被循环群的扩张等.) 由于这个问题异常困难，在本节中我们不想涉及这个问题. 尽管为了研究可裂扩张的需要，我们引进扩张函数等价的概念，并对 N 被 F 的两个扩张 N- 同构的条件作些讨论.

现在设 G 是 N 被 F 的一个给定的扩张， $\sigma: F\to G/N$ 是一给定的同构映射. 由定理 3.2 知，取定 N 的一组陪集代表

$\{\bar{x} \mid x \in F\}$ 我们可得到满足 (3.2) 式的一对扩张函数 $f(x,y)$ 和 $\alpha(x)$. 如果我们更换一组陪集代表 $\{\tilde{x} \mid x \in F\}$, 得到的扩张函数也要改变, 譬如变为 $f_1(x,y)$ 和 $\alpha_1(x)$. 假定两组陪集代表之间的关系是

$$\tilde{x} = \bar{x}\varphi(x), \text{ 其中} \varphi(x) \in N,$$

这样我们得到一个函数 $\varphi: F \to N$. 因为也要求 $\tilde{1} = 1$, 故 $\varphi(1) = 1$. 由直接计算易得 f, α 和 f_1, α_1 的关系为

$$\left.\begin{array}{l} f_1(x,y) = \varphi(xy)^{-1} f(x,y) \varphi(x)^{\alpha(y)} \varphi(y), \\ \alpha_1(x) = \alpha(x)\varphi(x), \end{array}\right\} \tag{3.5}$$

计算从略. 由上述讨论我们可以给出下面的

定义 3.3 称 N 被 F 的两个扩张 $G = \mathrm{Ext}(N, F; f, \alpha)$ 和 $G_1 = \mathrm{Ext}(N, F; f_1, \alpha_1)$ 为等价的, 如果存在函数 $\varphi: F \to N$, 能使 $\varphi(1) = 1$ 且 f, α, f_1, α_1 满足条件 (3.5). 我们也称这样的两对扩张函数 f, α 和 f_1, α_1 为等价的扩张函数.

定理 3.4 两个 N 被 F 的扩张 $G = \mathrm{Ext}(N, F; f, \alpha)$ 和 $G_1 = \mathrm{Ext}(N, F; f_1, \alpha_1)$ 等价, 则 G 和 G_1 必 N- 同构, 即存在同构 $\eta: G \to G_1$ 使 η 在 N 上的限制 $\eta|_N$ 为 N 的恒等同构.

证 因为 $G = \mathrm{Ext}(N, F; f, \alpha)$, $G_1 = \mathrm{Ext}(N, F; f_1, \alpha_1)$, 可令 $G = \{\bar{x}a \mid x \in F, a \in N\}$, $G_1 = \{\tilde{x}a \mid x \in F, a \in N\}$, 并且其中乘法运算为

$$\begin{aligned} \bar{x}a\bar{y}b &= \overline{xy} f(x,y) a^{\alpha(y)} b, \\ \tilde{x}a\tilde{y}b &= \widetilde{xy} f_1(x,y) a^{\alpha_1(y)} b. \end{aligned}$$

又因 G, G_1 等价, 故存在 $\varphi: F \to N$ 使 $\varphi(1) = 1$ 且成立 (3.5) 式. 现在我们如下规定 G_1 到 G 的映射 η:

$$\eta: \tilde{x}a \mapsto \bar{x}\varphi(x)a, \ \forall x \in F, a \in N.$$

我们要来证明 η 是 G_1 到 G 的 N- 同构. 首先由定义有 $\tilde{x}\varphi(x)^{-1}a$ 映到 $\bar{x}a$, 故 η 是满射; 又若 $\bar{x}\varphi(x)a=1$, 则 $x=1$, $\varphi(x)a=1$, 而因 $\varphi(1)=1$, 又有 $a=1$, 即 $\mathrm{Ker}\,\eta=\tilde{1}1=1$, 故 η 又是单射, 于是只要再验证 η 保持运算, 就得 η 是同构. 这可如下看出:

$$\begin{aligned}\eta(\tilde{x}a\tilde{y}b) &= \eta(\widetilde{xy}f_1(x,y)a^{\alpha_1(y)}b)\\ &= \overline{xy}\varphi(xy)f_1(x,y)a^{\alpha_1(y)}b\\ &= \overline{xy}f(x,y)\varphi(x)^{\alpha(y)}\varphi(y)a^{\alpha(y)\varphi(y)}b \text{ (用 (3.5) 式)}\\ &= \overline{xy}f(x,y)\varphi(x)^{\alpha(y)}a^{\alpha(y)}\varphi(y)b\\ &= \overline{xy}f(x,y)(\varphi(x)a)^{\alpha(y)}\varphi(y)b\\ &= \bar{x}\varphi(x)a\cdot\bar{y}\varphi(y)b\\ &= \eta(\tilde{x}a)\eta(\tilde{y}b).\end{aligned}$$

最后, 因 $\eta(\tilde{1}a)=\bar{1}\varphi(1)a=\bar{1}a$, 知 $\eta|_N=1_N$. 定理证毕. □

这个定理给出了 N 被 F 的两个扩张 N- 同构的充分条件. 事实上, 两个扩张 N- 同构的充要条件也不难得到, 因为它和以下的叙述无关, 我们不在这里讲述了. 有兴趣的读者可参看其他讲扩张理论的群论教科书, 或者作为练习自己推导一下. 但应注意 N- 同构和同构这两个概念是不同的. 容易找到例子说明两个扩张不 N- 同构, 但作为抽象群是同构的.

下面我们来讲述一类特殊的扩张 —— 可裂扩张. 为此先引进下面的

定义 3.5 设 N 是群 G 的子群, 称 N 在 G 中有 *补*, 如果存在 G 的子群 K 使 $G=NK$, 并且 $N\cap K=1$. 这时 K 叫做 N 在 G 中的 *补群*.

设 $G=\mathrm{Ext}(N,F;f,\alpha)$. 假定 N 在 G 中有补 $\tilde{F}$, 则显然有 $\tilde{F}\cong F$. 若取 $\tilde{F}$ 的元素作为 N 在 G 中的一个陪集代表系, 并设 $x\mapsto\tilde{x}$ 是 F 到 $\tilde{F}$ 的同构映射, 则由 $\{\tilde{x}\}$ 得到的扩张函数 f_1,α_1 应满足

$$f_1(x,y)=1,\ \forall x,y\in F.$$

并且 α_1 是 F 到 $\mathrm{Aut}(G)$ 的同态. 反过来容易证明, 如果扩张 $G = \mathrm{Ext}(N,F;f,\alpha)$ 与 $G_1 = \mathrm{Ext}(N,F;f_1,\alpha_1)$ 等价, 且 $f_1(x,y)=1$, α_1 是同态, 则 N 在 G 中必有补. 这是因为这时存在函数 $\varphi: F \to N$ 满足 $\varphi(1)=1$, 且 (3.5) 式成立, 于是有

$$\begin{aligned}
\bar{x}\varphi(x)\bar{y}\varphi(y) &= \overline{xy}f(x,y)\varphi(x)^{\alpha(y)}\varphi(y)\\
&= \overline{xy}\varphi(xy)[\varphi(xy)^{-1}f(x,y)\varphi(x)^{\alpha(y)}\varphi(y)]\\
&= \overline{xy}\varphi(xy)f_1(x,y)\\
&= \overline{xy}\varphi(xy),
\end{aligned}$$

故 $\{\bar{x}\varphi(x) \mid x \in F\}$ 为一与 F 同构的子群 $\tilde{F}$. 又

$$\tilde{F} \cap N = \{\bar{1}\varphi(1)\} = 1,$$

故 $\tilde{F}$ 是 N 在 G 中的补. 于是我们可给出下面的定义和定理.

定义 3.6 称扩张 $G = \mathrm{Ext}(N,F;f,\alpha)$ 为 *可裂的*, 如果它等价于 $\mathrm{Ext}(F,N;f_1,\alpha_1)$, 其中 $f_1(x,y)=1$, $\forall x,y \in F$, 且 α_1 是 F 到 $\mathrm{Aut}(G)$ 的同态.

定理 3.7 *下列事项等价:*

(1) 扩张 $G = \mathrm{Ext}(N,F;f,\alpha)$ 可裂;

(2) N 在 G 中有补;

(3) 存在函数 $\varphi: F \to N$, $\varphi(1)=1$, 并使

$$f(x,y) = \varphi(xy)\varphi(y)^{-1}\varphi(x)^{-\alpha(y)}, \ \forall x,y \in F.$$

N 被 F 的可裂扩张也叫 N *和* F *的半直积*. 由于可裂扩张可选扩张函数 $f=1$, 故为确定半直积, 只须指明映射 α 即可. 并且相应于 $f=1$, α 是 F 到 $\mathrm{Aut}(G)$ 内的同态. 因为半直积在构造群例时十分有用, 而且它完全可以不借助扩张理论来讲述. 我们再给出下面的

定义 3.8 设 N, F 为两个抽象群. $\alpha: F \to \mathrm{Aut}(N)$ 是同态映射, 则 N *和* F *关于* α *的半直积* $G = N \rtimes_\alpha F$ 规定为

$$G = F \times N = \{(x,a) \mid x \in F, a \in N\},$$

运算为

$$(x,a)(y,b)=(xy,a^{\alpha(y)}b);$$

或者

$$G=N\times F=\{(a,x)\mid a\in N,x\in F\},$$

运算为

$$(a,x)(b,y)=(ab^{\alpha(x)^{-1}},xy).$$

可用扩张理论证明，或者直接验证如上规定的半直积确实成群，并且两种形式规定的半直积是同构的．（因此我们在符号上不加区别，都用 G 表示．）若把 F,N 分别与 $\{(x,1)\mid x\in F\}$, $\{(1,a)\mid a\in N\}$（或者 $\{(1,x)\mid x\in F\}$, $\{(a,1)\mid a\in N\}$）等同看待，则 $G=NF=FN$, 且 $N\cap F=1$.

对于半直积 $G=N\rtimes_\alpha F$, 若取 $\alpha=0$, 即对每个 $x\in F$, $\alpha(x)$ 都是 N 的恒等映射，则 G 就变成 N 和 F 的直积.

下面我们再来看群扩张的另外两种特殊情形，它们对研究有限群的构造也十分有用.

首先，如果 N 是交换群，则由 (3.2) 式，由 N 被 F 的任意扩张得到的扩张函数中的 α 恒满足

$$\alpha(x)\alpha(y)=\alpha(xy),\ \forall x,y\in F,$$

即 α 是 F 到 $\mathrm{Aut}(N)$ 内的同态．这是因为由 N 的任意元素诱导出的 N 的自同构显然均为恒等自同构.

下节我们将应用这个性质来证明对有限群十分重要的 Schur-Zassenhaus 定理.

另一种特情形是群 N 的有限循环扩张, 即当 F 为有限循环群时 N 被 F 的扩张．设 F 为 m 阶循环群，由 s 生成:

$$F=\langle s\rangle=\{1,s,\cdots,s^{m-1}\}.$$

仍设 G 为 N 被 F 的扩张．假定在同构 $\sigma:F\to G/N$ 之下 s 的像为 $\bar{s}N$, $\bar{s}$ 是陪集 $\bar{s}N$ 中任一选定的代表元，则 G 对 N 的陪集分解式可设为

$$G=N\cup\bar{s}N\cup\bar{s}^2N\cup\cdots\cup\bar{s}^{m-1}N, \tag{3.1'}$$

并有 $\bar{s}^m \in N$. 令 $\bar{s}^m = a$, 则扩张函数 f 有形状

$$f(s^i, s^j) = \begin{cases} 1, & i+j < m, \\ a, & i+j \geq m. \end{cases} \tag{3.6}$$

又设 $\alpha(s) = \tau \in \mathrm{Aut}(N)$, 则函数 α 有形状

$$\alpha(s^i) = \tau^i,\ i = 0, 1, \cdots, m-1. \tag{3.7}$$

由 (3.2) 式可得到

$$a^\tau = a,\ \tau^m = a. \tag{3.2'}$$

这只要在 (3.2) 式中令 $x = s$, $y = s^{m-1}$, $z = s$ 即可得到上式.

反过来，如果给了满足 (3.2′) 式的 $a \in N$ 和 $\tau \in \mathrm{Aut}(N)$, 则由 (3.6) 及 (3.7) 规定的扩张函数 f, α 就满足 (3.2) 式 (验证从略), 于是也就确定一个 N 被 m 阶循环群 F 的扩张. 这样我们得到下面的

定理 3.9 设 N 是群, $F = \langle s \rangle$ 是 m 阶循环群. 又设 $a \in N$, $\tau \in \mathrm{Aut}(N)$, a 与 τ 满足 (3.2′) 式. 则由 (3.6) 及 (3.7) 式确定的 f 和 α 满足 (3.2) 式. 因而可得一 N 被 F 的扩张 G(简称 N 的 m 次循环扩张), 记作 $G = \mathrm{Ext}(N, m; a, \tau)$. 并且 N 的所有 m 次循环扩张均可由适当的满足 (3.2′) 式的 a, τ 依上法得到.

这个定理给出了决定群 N 的所有循环扩张的方法. 但对于不同的 a, τ 确定的扩张何时同构的问题并没有回答.

循环群被循环群的扩张是更特殊的情形. 我们先有

定义 3.10 称 G 为 亚循环群, 如果 G 有循环正规子群 N, 使商群 G/N 也是循环群. 即, 亚循环群为循环群被循环群的扩张.

下面的 Hölder 定理决定了有限亚循环群的构造.

定理 3.11 设 $n, m \geq 2$ 为正整数, G 是 n 阶循环群 N 被 m 阶循环群 F 的扩张. 则 G 有如下定义关系:

$$G = \langle u, v \rangle,\ u^n = 1, v^m = u^t, v^{-1}uv = u^r, \tag{3.8}$$

其中参数 n, m, t, r 满足关系式

$$r^m \equiv 1 \pmod{n}, \ t(r-1) \equiv 0 \pmod{n}. \tag{3.9}$$

反之, 对每组满足 (3.9) 式的参数 n, m, t, r, (3.8) 式都确定一个 n 阶循环群被 m 阶循环群的扩张.

证 设 G 是一个这样的扩张, 可令 $G = \mathrm{Ext}(N, m; a, \tau)$, 其中 $N = \langle u \rangle$, $u^n = 1$; $a = u^t$, τ 由 $u^\tau = u^r$ 确定, 并且 a, τ 满足条件 (3.2′). 再设 G 关于 N 的左陪集分解式为

$$G = N \cup vN \cup v^2 N \cup \cdots \cup v^{m-1} N,$$

(参看 (3.1′) 式), 我们有 $v^m = u^t$, $v^{-1}uv = u^r$. 于是对于 G 关系式 (3.8) 成立. 而由条件 (3.2′) 推出 $u^{tr} = u^t$ 和 $\tau^m = 1$ (由 N 交换). 由此又得 $r^m \equiv 1 \pmod{n}$ 和 $t(r-1) \equiv 0 \pmod{n}$, 此即条件 (3.9).

另外, 容易看出, 以条件 (3.8) 和 (3.9) 为定义关系的群的阶 $\leq mn$, 而 $|G| = mn$, 故 G 以 (3.8) 和 (3.9) 式为定义关系.

反过来, 容易直接验证或由定理 3.9 证明, 定义关系 (3.8) 和 (3.9) 式确定一 n 阶循环群被 m 阶循环群的扩张, 细节从略. □

对于亚循环群的同构分类问题已由 B.G. Basmaji 在 1969 年解决, 可参看下面的文章:

On the isomorphisms of two metacyclic groups, *Proc. Amer. Math. Soc.*, **22**(1969), 175–182.

最后, 我们举一个例子来说明前述理论如何用来解决比较简单的群的同构分类问题.

例 3.12 决定所有的 12 阶群.

解 首先, 由交换群分解定理, 12 阶交换群只有两种类型, 即 $Z_3 \times Z_4$ 和 $Z_3 \times Z_2 \times Z_2$. 故以下可假定该群 G 非交换. 这时 G 的 Sylow 2- 子群和 Sylow 3- 子群不能都在 G 中正规.

(1) 若 G 的 Sylow 3- 子群 H 非正规, 则显然 H 的核 $H_G = 1$, 于是 G 在 H 上的置换表示是 G 的忠实表示. 因为 $|G : H| = 4$,

有 $G \lesssim S_4$. 容易证明 S_4 中只有一个 12 阶子群 A_4 (请读者自证.) 于是有 $G \cong A_4$.

(2) 若 G 的 Sylow 3- 子群 H 在 G 中正规, 则 G 的 Sylow 2- 子群 S 不正规. 此时 $G = H \rtimes S$. 对子群 H 应用 N/C 定理, 有

$$G/C_G(H) \lesssim \mathrm{Aut}(H) \cong Z_2.$$

由 G 非交换, 只能有 $G/C_G(H) \cong Z_2$. 这时 $|C_G(H)| = 6$, 必有 $C_G(H) \cong Z_6$. 故 G 为 Z_6 被 Z_2 的扩张. 由定理 3.11, G 有定义关系:

$$u^6 = 1,\ v^2 = u^t,\ v^{-1}uv = u^r,$$

$$r \not\equiv 1 \pmod 6, r^2 \equiv 1 \pmod 6, t(r-1) \equiv 0 \pmod 6.$$

由上述同余式可解得 $r \equiv -1$, $t \equiv 3$ 或 $0 \pmod 6$. 这分别对应于 G 为 12 阶二面体群 D_{12} 和 12 阶广义四元数群. 又因为前者无 4 阶元, 后者有 4 阶元, 此二群不会同构.

总结一下, 12 阶群计有以下五种互不同构的类型:

(I) 交换群:

(1) $G \cong Z_3 \times Z_4$;

(2) $G \cong Z_6 \times Z_2$;

(II) 非交换群:

(3) $G \cong A_4$;

(4) $G = \langle u, v \rangle$, $u^6 = 1, v^2 = 1, v^{-1}uv = u^{-1}$;

(5) $G = \langle u, v \rangle$, $u^6 = 1, v^2 = u^3, v^{-1}uv = u^{-1}$.

§4. Schur-Zassenhaus 定理

有限群的 Sylow 子群的一个重要推广是所谓 Hall 子群. 为引进这个概念, 我们先规定一些符号.

我们常以 π 表示一个由素数组成的集合, 而以 π' 表示 π 在全体素数集合中的补集. 称群的元素 x 为一个 π- 元素 (或 π'- 元素), 如果 x 的阶 $o(x)$ 的素因子分解式中仅出现 π 中 (或 π' 中) 的素数. 设 N 是正整数, 我们以 N_π 表示能整除 N 并且素因子全

在 π 中的最大整数. 当 $\pi=\{p\}$, 我们记 N_π 为 N_p. 称群 G 为一个 π- 群, 如果 $|G|_\pi=|G|$.

定义 4.1 设 π 是一个素数集合. 称 G 的子群 H 为 G 的一个 π-Hall 子群, 如果 $|H|=|G|_\pi$. 而称 H 为 G 的 Hall 子群, 如果对某个素数集合 π 来说, H 是 G 的 π-Hall 子群.

等价地, H 是 G 的 Hall 子群, 如果 $(|H|,|G:H|)=1$.

由这个定义, Sylow p- 子群也是 Hall 子群, 它对应的素数集合 $\pi=\{p\}$.

命题 4.2 设 H 是 G 的 π-Hall 子群, $N\trianglelefteq G$, 则 HN/N 是 G/N 的 π-Hall 子群. 若又有 $H\trianglelefteq G, U\leq G$, 则 $U\cap H$ 是 U 的正规 π-Hall 子群.

证 因 $HN/N\cong H/H\cap N$, 故 $|HN/N|\mid|H|$. 又因 $|G/N:HN/N|=|G:HN|$ 可整除 $|G:H|$, 于是由 $(|H|,|G:H|)=1$ 得 $(|G/N:HN/N|,|HN/N|)=1$, 故 HN/N 是 G/N 的 Hall 子群. 又因 $|HN/N|_\pi=|H/H\cap N|_\pi=|H/H\cap N|=|HN/N|$, 故 HN/N 是 π- 群, 所以是 G/N 的 π-Hall 子群.

再假定 $H\trianglelefteq G$, 有 $HU/H\cong U/U\cap H$, 而 $|HU/H|$ 可整除 $|G/H|$, $|U\cap H|$ 可整除 $|H|$, 由 $(|H|,|G/H|)=1$ 得 $(|U/U\cap H|,|U\cap H|)=1$, 故 $U\cap H$ 是 U 的 π-Hall 子群. □

类似于 Sylow 定理, 我们要考虑 π-Hall 子群的存在性和共轭性等问题. 下面的 Schur-Zassenhaus 定理虽然只在一个特殊情形下回答了这个问题, 但它对研究这个问题具有基本的意义. 后面在第 V 章中, 我们还将继续讨论有限群的 π'-Hall 子群.

定理 4.3 (Schur-Zassenhaus) 设 N 是 G 的正规 Hall 子群, 则

(1) N 在 G 中有补;

(2) 若 N 或 G/N 可解, H 和 H_1 是 N 在 G 中的两个补群, 则存在 $u\in N$ 使 $H^u=H_1$.

注意，因 $(|N|,|G/N|)=1$，故 $|N|$ 和 $|G/N|$ 中至少有一个是奇数. 而由 Feit-Thompson 定理，奇数阶群必可解，于是 (2) 中的可解性条件恒满足.

为证明这个定理，我们先来证明一个引理，它是定理的特殊情形.

引理 4.4 *在定理 4.3 中补充假定 N 是交换群，则该定理成立.*

证 分下面两步：

(1) 证明 N 在 G 中有补：令 $F=G/N$，把 G 看作 N 被 F 的扩张，我们要证它是可裂的.

任取 N 的一组陪集代表 $\{\bar{x} \mid x\in F\}$，可得满足 (3.2) 式的扩张函数 f 和 α. 为证扩张是可裂的，根据定理 3.7，我们只须证存在函数 $\varphi: F\to N$，满足 $\varphi(1)=1$，并且

$$f(x,y)=\varphi(xy)\varphi(y)^{-1}\varphi(x)^{-\alpha(y)},\ \forall x,y\in F.$$

首先，由 (3.2) 式，对任意的 $x,y,z\in F$，有

$$f(xy,z)f(x,y)^{\alpha(z)}=f(x,yz)f(y,z).$$

取定 y,z，让 x 跑遍 F，并求积 (注意 N 是交换群)，得

$$\prod_{x\in F}f(xy,z)\prod_{x\in F}f(x,y)^{\alpha(z)}=\prod_{x\in F}f(x,yz)\cdot f(y,z)^{|F|}.$$

令 $\varphi_1(u)=\prod_{x\in F}f(x,u)$，则上式变为

$$\varphi_1(z)\varphi_1(y)^{\alpha(z)}=\varphi_1(yz)f(y,z)^{|F|}. \tag{4.1}$$

因为 $(|F|,|N|)=1$，故有整数 r 使 $r|F|\equiv 1 \pmod{|N|}$，于是 $f(y,z)^{-r|F|}=f(y,z)^{-1}$. 令 $\varphi(u)=\varphi_1(u)^{-r}$，则由 (4.1) 式可得

$$\varphi(z)\varphi(y)^{\alpha(z)}=\varphi(yz)f(y,z)^{-1}.$$

把 y,z 代之以 x,y, 即得

$$f(x,y)=\varphi(xy)\varphi(y)^{-1}\varphi(x)^{-\alpha(y)}.$$

又, $\varphi(1)=\varphi_1(1)^{-r}=\prod_{x\in F}f(x,1)^{-r}=1$. 故 φ 满足我们的要求.

(2) 设 H,H_1 是 N 在 G 中的两个补群, 证明存在 $u\in N$ 使 $H^u=H_1$: 令在 H 和 H_1 中对应于 $F=G/N$ 中元素 x 的元素分别为 $\bar{x}\in H$ 和 $\tilde{x}\in H_1$, 这时有 $\bar{x}N=\tilde{x}N$, 故可设 $\tilde{x}=\bar{x}\psi(x)$, 其中 $\psi(x)\in N$. 因为 $\tilde{x}\tilde{y}=\widetilde{xy}$, 有

$$\bar{x}\psi(x)\bar{y}\psi(y)=\overline{xy}\psi(xy),$$

即

$$\bar{x}\bar{y}\psi(x)^{\bar{y}}\psi(y)=\overline{xy}\psi(xy).$$

又由 $\bar{x}\bar{y}=\overline{xy}$, 得

$$\psi(x)^{\bar{y}}\psi(y)=\psi(xy).$$

固定元素 y, 让 x 跑遍 F, 并求积得

$$\prod_{x\in F}\psi(x)^{\bar{y}}\cdot\psi(y)^{|F|}=\prod_{x\in F}\psi(xy).$$

令 $z=\prod_{x\in F}\psi(x)$, 得

$$z^{\bar{y}}\psi(y)^{|F|}=z.$$

仍取 r 满足 $r|F|\equiv 1 \pmod{|N|}$, 并令 $u=z^r$, 有

$$u^{\bar{y}}\psi(y)=u,$$

即 $u=\bar{y}^{-1}u\bar{y}\psi(y)$, 于是得

$$u^{-1}\bar{y}u=\bar{y}\psi(y)=\tilde{y},\ \forall y\in F,$$

即 $H^u=H_1$. 又因 $u\in N$, 引理得证. □

定理 4.3 的证明: 亦分为下面两步:

(1) 证 N 在 G 中补群的存在性:

设 $|N|=n$, 用对 n 的归纳法. 当 $n=1$ 时显然, 故设 $n>1$. 假定素数 $p \mid n$, 则 G 的每个 Sylow p- 子群皆在 N 中. 设 P 是 G 的一个 Sylow p- 子群, 当然它也是 N 的 Sylow p- 子群. 令 $N_p=N_G(P)$. 由 Frattini 论断, $G=N_pN$. 于是有

$$G/N=N_pN/N \cong N_p/N_p \cap N \cong (N_p/P) \,/\, (N_p \cap N/P).$$

因为 $|N_p \cap N/P| \mid |N|$, 故在 N_p/P 中, $N_p \cap N/P$ 的阶与其指数互素, 即 $N_p \cap N/P$ 是 N_p/P 的正规 Hall 子群. 又显然 $|N_p \cap N/P| < |N|$, 由归纳假设, $N_p \cap N/P$ 在 N_p/P 中有补 U/P, 且 $|U/P|=|G/N|$.

再令 $Z=Z(P)$, 有 $Z \neq 1$ 并且 Z char P. 于是 $Z \trianglelefteq U$. 考虑 U/Z, 它有正规 Hall 子群 P/Z. 显然 $|P/Z|<|N|$, 又由归纳假设, P/Z 在 U/Z 中有补 V/Z, 且 $|V/Z|=|U/P|=|G/N|$. 此时因 Z 是交换群, 由引理 4.4, Z 在 V 中有补 H, 并且 $|H|=|G/N|$, 于是 H 也是 N 在 G 中的补群.

(2) 设 H, H_1 是 N 在 G 中的两个补群, 证明存在 $u \in N$ 使 $H^u=H_1$. 分两种情形:

(i) 假定 N 是可解群: 设 N 的导列长为 k. 若 $k=1$, N 是交换群. 由引理 4.4, 结论成立. 故可设 $k>1$. 用对 k 的归纳法. 因 N 的导群 $N' \trianglelefteq G$, 考虑 G/N'. 这时 N/N' 是 G/N' 的正规 Hall 子群, HN'/N' 和 H_1N'/N' 是 N/N' 的两个补群. 再因 N/N' 交换, 由引理 4.4, 存在 $x \in N$ 使 $H^xN'=H_1N'$. 考虑 H_1N', 有 H_1 和 H^x 是 N' 在其中的两个补群. 而 N' 的导列长 $=k-1<k$, 故由归纳假设, 存在 $y \in N'$ 使 $H^{xy}=H_1$. 令 $u=xy$, 有 $u \in N$, 并且 $H^u=H_1$.

(ii) 假定 G/N 是可解群: 因 $H \cong G/N \cong H_1$, 知 N 的所有补群均同构. 设 H 的主群列长度为 l, 对 l 用归纳法.

当 $l=1$ 时, H 是初等交换 p- 群 (实际上是 p 阶循环群). 因 H, H_1 都是 G 的 Sylow p- 子群, 存在 $g \in G$ 使 $H^g=H_1$. 又因 $G=HN$, 故 $g=hu$, 其中 $h \in H$, $u \in N$. 于是 $H^g=H^{hu}=H^u=H_1$.

设 $l > 1$, 令 T 是 H 的一个极小正规子群. 由 H 可解, 对于某个素数 p, T 必为初等交换 p- 群. 这时有 $TN \trianglelefteq HN = G$. 令 $T_1 = H_1 \cap TN$, 有 $T_1 \trianglelefteq H_1$, 并且因

$$\begin{aligned} H/T &= H/H \cap TN \cong HTN/TN = G/TN \\ &= H_1TN/TN \cong H_1/T_1, \end{aligned}$$

有 $|T_1| = |T|$, 于是 $T_1N = TN$. 因 T 和 T_1 是 N 在 TN 中的补群, 并且都是 TN 的 Sylow p- 子群, 与前面相同, 可证明存在 $x \in N$ 使 $T_1 = T^x$. 这样 H^x 和 H_1 均包含 T_1 作为其正规子群. 于是有 $M = N_G(T_1) \geq H^x$, $M \geq H_1$. 根据命题 4.2, $N \cap M$ 是 M 的正规 Hall 子群. 由此得 $(N \cap M)T_1/T_1 \trianglelefteq M/T_1$, 并且有补群 H_1/T_1 和 H^x/T_1. 由 H_1/T_1 的主群列长度 $< l$, 推出存在 $y \in N \cap M$ 使 $H^{xy} = H_1$. 令 $u = xy$, 则有 $u \in N$, 并且 $H^u = H_1$. 定理证毕. □

注 4.5 前面已经看出, 由 Feit-Thompson 定理, 在定理 4.3 中假定 N 或 G/N 可解是多余的. 但去掉这个假定, 如何给出一个不依赖于 Feit-Thompson 定理的证明则是一件十分吸引人的工作, 但至今尚未成功. 曾经有人应用 Schreier 猜想给出了一个证明, 可见研究题 10.

又, 对于 N 是交换群的情形, W. Gaschütz 曾把定理 4.3 推广为

定理 4.6 *设 G 是有限群, $N \trianglelefteq G$, N 交换. 又 $N \leq M \leq G$, $(|N|, |G:M|) = 1$. 则有*

(1) 若 N 在 M 中有补, 则 N 在 G 中也有补;

(2) 若 N 在 M 中有补, 且所有这样的补全在 M 中共轭, 则所有 N 在 G 中的补也在 G 中共轭.

由此定理还可推出下面的

推论 4.7 *设 N 是 G 的交换正规子群, 则 N 在 G 中有补的充要条件为对于 G 的每个 Sylow 子群 S, $S \cap N$ 在 S 中也有补.*

定理 4.6 的证明使用了群的上同调方法，这在本书中不拟介绍．有兴趣的读者可参看 B. Huppert 的 “Endliche Gruppen I” 中 I,17.4.

§5. 圈积、对称群的 Sylow 子群

定义 5.1 设 G 是群， H 是有限集合 Ω 上的置换群．为简便计，令 $\Omega = \{1, 2, \cdots, n\}$．再设 N 是 G 的 n 次直接幂，即 n 个 G 的 (外) 直积：

$$N = \underbrace{G \times \cdots \times G}_{n\text{个}}.$$

对于任意的 $h \in H$，容易验证如下规定的映射 $\alpha(h)$ 是 N 的一个自同构：

$$(g_1, \cdots, g_n)^{\alpha(h)} = (g_{1^{h^{-1}}}, \cdots, g_{n^{h^{-1}}}),\ g_i \in G,\ i = 1, \cdots, n,$$

并且满足 $\alpha(hh') = \alpha(h)\alpha(h')$, $\forall h, h' \in H$．这样 $\alpha : H \to \mathrm{Aut}(N)$ 是同态．[2] 据定义 3.8，作 N 和 H 关于 α 的半直积 $N \rtimes_\alpha H$，叫做 G 和 H 的 圈积，记作 $G \wr H$．如果明确写出，即

$$G \wr H = \{(g_1 \cdots, g_n; h) \mid g_i \in G, h \in H\},$$

其中乘法如下规定：

$$(g_1 \cdots, g_n; h)(g_1' \cdots, g_n'; h') = (g_1 g'_{1^h} \cdots, g_n g'_{n^h}; hh').$$

[2]为真正弄清圈积的构造，请读者务必仔细验证并搞清 α 为什么是 H 到 $\mathrm{Aut}(N)$ 内的同态．注意，如果对任意的 $h \in H$，如下规定映射 $\beta(h)$:

$$(g_1, \cdots, g_n)^{\beta(h)} = (g_{1^h}, \cdots, g_{n^h}),\ g_i \in G,\ i = 1, \cdots, n,$$

则 $\beta(h)$ 亦为 N 的自同构．但 β 却不是 H 到 $\mathrm{Aut}(N)$ 内的同态，而是反同态．即满足

$$\beta(hh') = \beta(h')\beta(h),\ \forall h, h' \in H.$$

根据这个定义，一个抽象群 G 和一个有限置换群 H 的圈积 $G\wr H$ 是一个抽象群. 又显然有

命题 5.2 若 G 也是有限群，则

$$|G\wr H| = |G|^n|H|.$$

注 5.3 容易验证，在圈积 $G\wr H$ 中，

$$\tilde{G} = \{(g,1,\cdots,1;1) \mid g\in G\}$$

和

$$\tilde{H} = \{(1,1,\cdots,1;h) \mid h\in H\}$$

分别为 $G\wr H$ 的同构于 G 和 H 的子群. 如果把 $G,\tilde{G}$ 以及 $H,\tilde{H}$ 等同看待，可认为 G,H 都是 $G\wr H$ 的子群，并且有 $G\wr H=\langle G,H\rangle$. (证明留给读者作为习题).

注 5.4 如果在定义 5.1 中，又假定 G 是有限集合 Δ 上的置换群，则可依下述方式把圈积 $G\wr H$ 看作 $\Delta\times\Omega$ 上的置换群：对于 $\delta\in\Delta$, $i\in\Omega$, 规定

$$(\delta,i)^{(g_1,\cdots,g_n;h)} = (\delta^{g_i}, i^h).$$

这时我们有圈积的结合律：

命题 5.5 设 G,H,K 分别为集合 Δ,Ω,Γ 上的置换群. 则 $(G\wr H)\wr K$ 和 $G\wr(H\wr K)$ 分别可看作集合 $(\Delta\times\Omega)\times\Gamma$ 和 $\Delta\times(\Omega\times\Gamma)$ 上的置换群. 且若把 $(\Delta\times\Omega)\times\Gamma$ 和 $\Delta\times(\Omega\times\Gamma)$ 等同看待，都看成是 $\Delta\times\Omega\times\Gamma$, 有

$$(G\wr H)\wr K = G\wr(H\wr K).$$

证 由注 5.4 得命题的前半部分. 为证命题的后半部分，不失普遍性可设 $\Delta=\{1,2,\cdots,m\}$, $\Omega=\{1,2,\cdots,n\}$, $\Gamma=\{1,2,\cdots,s\}$. 对于 $(G\wr H)\wr K$ 中的任意元素

$$x = (g_{11},\cdots,g_{n1};h_1;g_{12},\cdots,g_{n2};h_2;\cdots;g_{1s},\cdots,g_{ns};h_s;k),$$

其中 $g_{ir} \in G, h_r \in H, k \in K$; $i = 1, \cdots, n; r = 1, \cdots, s$, 相应地，在 $G \wr (H \wr K)$ 中有元素

$$y = (g_{11}, \cdots, g_{n1}, g_{12}, \cdots, g_{n2}, \cdots, g_{1s}, \cdots, g_{ns}; h_1, \cdots, h_s; k),$$

反之亦然. 由直接验证知， x 和 y 作为 $\Delta \times \Omega \times \Gamma$ 上的置换是相等的. 这因为，对于 $\Delta \times \Omega \times \Gamma$ 的任意元素 (δ, i, r), $\delta \in \Delta$, $i \in \Omega$, $r \in \Gamma$, 有

$$\begin{aligned}
(\delta, i, r)^x &= ((\delta, i)^{(g_{1r}, \cdots, g_{nr}; h_r)}, r^k) \\
&= (\delta^{g_{ir}}, i^{h_r}, r^k), \\
(\delta, i, r)^y &= (\delta^{g_{ir}}, (i, r)^{h_1, \cdots, h_r; k}) \\
&= (\delta^{g_{ir}}, i^{h_r}, r^k).
\end{aligned}$$

于是 $(\delta, i, r)^x = (\delta, i, r)^y$, $\forall \delta \in \Delta, i \in \Omega, r \in \Gamma$. 即 $x = y$. 于是得

$$(G \wr H) \wr K = G \wr (H \wr K).$$

□

下面我们讨论对称群 S_n 的 Sylow p- 子群. 设 $P \in \mathrm{Syl}_p(S_n)$, 则 $|P| = |S_n|_p = (n!)_p$. 令 $|P| = p^{s(n)}$, 则由初等数论知

$$s(n) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots,$$

其中 $[a]$ 表示实数 a 的整数部分. 现在令

$$n = a_r p^r + a_{r-1} p^{r-1} + \cdots + a_1 p + a_0,$$

其中 $0 \le a_i \le p-1$, $i = 0, 1, \cdots, r$, 且 $a_r \ne 0$. 则容易验证

$$s(n) = a_r s(p^r) + a_{r-1} s(p^{r-1}) + \cdots + a_1 s(p) + a_0 s(1).$$

这样，欲求 S_n 的 Sylow p- 子群，只要把 n 个文字如下分组，使得有 a_r 组每组包含 p^r 个文字， a_{r-1} 组每组包含 p^{r-1} 个文字，

$\cdots, a_1$ 组每组包含 p 个文字, a_0 组每组包含 1 个文字. 如果对于每一组, 譬如含 p^i 个文字的, 我们能求出作用在它们上的一个 $p^{s(p^i)}$ 阶子群, 即作用在它们上面的对称群的 Sylow p- 子群. 那么, 我们把所有这些子群 (均看成是作用在全部 n 个文字上的) 作直积即得到 S_n 的一个 $p^{s(n)}$ 阶子群, 它就是 S_n 的一个 Sylow p- 子群. 用这种办法, 我们把问题化归为 n 是 p 的方幂的情形. 而下面的定理又解决了这个问题.

定理 5.6 设 Z_p 是 $\Omega = \{1, 2, \cdots, p\}$ 上的 p 阶循环置换群, 则

$$P = \underbrace{Z_p \wr Z_p \wr \cdots \wr Z_p}_{r\text{个}}$$

看作 p^r 个文字的集合 $\Gamma = \underbrace{\Omega \times \Omega \times \cdots \times \Omega}_{r\text{个}}$ 上的置换群, 其阶为 $p^{s(p^r)}$, 因此是 S_Γ 的 Sylow p- 子群.

证 由命题 5.5, 置换群的圈积成立结合律, 故 $P = Z_p \wr Z_p \wr \cdots \wr Z_p$ 是有意义的, 并可看作是 Γ 上的置换群. 由命题 5.2, 计算得

$$|P| = p^{p^{r-1}+p^{r-2}+\cdots+1} = p^{s(p^r)}.$$

因为 S_Γ 的 Sylow p- 子群的阶应为 $p^{s(p^r)}$, 与 $|P|$ 相等, 故 $P \in \mathrm{Syl}_p(S_\Gamma)$. □

至此我们已经弄清对称群的 Sylow p- 子群的构造, 下面再给一个具体的例子.

例 5.7 设 p 是素数, $\Delta = \{1, 2, \cdots, p^2\}$. 试写出 S_Δ 的 Sylow p- 子群的生成元.

解 令 $\Omega = \{1, 2, \cdots, p\}$, 则 $Z_p = \langle a \rangle$, $a = (1\ 2 \cdots\ p)$, 是 S_Ω 的 Sylow p- 子群. 再令 $\Gamma = \Omega \times \Omega$. 由定理 5.6, $P = Z_p \wr Z_p$ 是 S_Γ 的 Sylow p- 子群. 据注 5.3, $P = \langle x, y \rangle$, 其中 $x = (a, 1, \cdots, 1; 1)$,

$y=(1,1,\cdots,1;a)$. 具体写出 x 和 y 在 Γ 上的作用如下：对 $i,j=1,2,\cdots,p$, 有

$$(i,j)^x=\begin{cases}(i^a,j), & j=1\\(i,j), & j\neq 1;\end{cases}$$

$$(i,j)^y=(i,j^a).$$

因映射 $(i,j)\mapsto i+pj-p$ 是 Γ 到 Δ 上的一一映射，易看出若把 x,y 看成是 Δ 上的置换应有下列形状的轮换分解式：

$$\begin{aligned}x &= (1\ 2\ \cdots\ p),\\ y &= (1\ 1+p\ \cdots\ 1+p^2-p)(2\ 2+p\ \cdots\ 2+p^2-p)\cdots\\ &\quad (p\ 2p\ \cdots\ p^2).\end{aligned}$$

□

§6. $\mathcal{P}$ 临界群

我们以 $\mathcal{P}$ 表示任一群性质，比如可解，交换，循环等等. 称群 G 为 $\mathcal{P}$ 群，如果 G 具有性质 $\mathcal{P}$.

定义 6.1 设 $\mathcal{P}$ 是任一群性质，称 $\mathcal{P}$ 是*子群遗传的*，如果由任一群 G 是 $\mathcal{P}$ 群可推出 G 的任一子群 H 也是 $\mathcal{P}$ 群；而称 $\mathcal{P}$ 是*商群遗传的*，如果由任一群 G 是 $\mathcal{P}$ 群可推出 G 的任一商群 G/N 也是 $\mathcal{P}$ 群.

前面提到的群的可解性，交换性和循环性都是子群遗传和商群遗传的.

我们称群 G 的任一子群的商群为 G 的一个*截段*. 于是若 $\mathcal{P}$ 同时为子群遗传和商群遗传的，则由 G 是 $\mathcal{P}$ 群可推出 G 的任一截段也是 $\mathcal{P}$ 群.

当然有很多群性质既非子群遗传也非商群遗传. 例如以 $\mathcal{P}$ 代表有限群的阶可被某指定的素数 p 整除的性质，则 $\mathcal{P}$ 显然既非子群遗传也非商群遗传，因为单位元群是任一群的子群和商群，但

它的阶不能被 p 整除. 也有些性质是子群遗传的但非商群遗传, 或者是商群遗传但非子群遗传, 请读者自己举些例子来说明.

在研究群性质 $\mathcal{P}$ 时, 特别是为建立 $\mathcal{P}$ 群的充分条件, 下面的几种所谓 $\mathcal{P}$ 临界群的概念将起着重要的作用.

定义 6.2 设 $\mathcal{P}$ 为一子群遗传的群性质, 群 G 不是 $\mathcal{P}$ 群, 但 G 的每个真子群皆为 $\mathcal{P}$ 群, 则称 G 为一个 *内 $\mathcal{P}$ 群*.

定义 6.3 设 $\mathcal{P}$ 为一商群遗传的群性质, 群 G 不是 $\mathcal{P}$ 群, 但 G 的每个真商群皆为 $\mathcal{P}$ 群, 则称 G 为一个 *外 $\mathcal{P}$ 群*.

定义 6.4 设 $\mathcal{P}$ 为一子群遗传同时又商群遗传的群性质, 群 G 不是 $\mathcal{P}$ 群, 但 G 的每个真子群和每个真商群皆为 $\mathcal{P}$ 群, 则称 G 为 *一个极小非 $\mathcal{P}$ 群*.

应该注意, 在多数群论文献中使用的术语和我们这里的不太一样. 他们一般只用 "极小非 $\mathcal{P}$ 群" 的术语, 多数情形下指的是 "内 $\mathcal{P}$ 群", 有时也用来代表 "外 $\mathcal{P}$ 群" 和 "极小非 $\mathcal{P}$ 群", 请读者在阅读文献时加以注意.

下面我们举几个简单的例子来说明 $\mathcal{P}$ 临界群的概念在研究群性质 $\mathcal{P}$ 时的作用. 在本书的以后各章, 还将多次应用这个概念.

首先看一个如何用内交换群来研究群的交换性的例子. 对于内交换群的性质和构造早在 1903 年就已经得到, 可见下列文章:

G.A. Miller and H.C. Moreno, Non-abelian groups in which every subgroup is abelian, *Trans. Amer. Math. Soc.*, 4(1903), 398–404.

但我们这里只用到内交换群的可解性, 即

定理 6.5 *有限内交换群 G 必为可解群.*

证 由 I,7.10 知, 有限内交换群必含非平凡正规子群, 我们应用这点来证明它的可解性.

取 G 的极大正规子群 N, 即使 G/N 为单群者. 由 G 的内交换性, N 是交换群. 如果 G/N 亦交换, 则已可得 G 可解. 而若 G/N 非交换, 设 M/N 为其任一极大子群, 则 M 亦为 G 之极大子群, 又由 G 内交换, 得 M 交换, 于是 M/N 交换. 这说明 G/N 也是内交换群. 但 G/N 又是单群, 与 I,7.10 矛盾. 证毕. □

下面应用定理 6.5 证明 Zassenhaus 定理, 即 I,7.11.

定理 6.6 设 G 是有限群, 对于它的每个交换子群 A 恒有 $C_G(A) = N_G(A)$. 则 G 本身交换.

证 首先, 易验证定理条件是子群遗传的. 于是, 若定理不真, 极小反例 G 必为内交换群. 由定理 6.5 G 可解. 取 G 之极大正规子群 N, 得 N 交换, 且 $|G:N|$ 为素数. 由 G 非交换, 得 $C_G(N) = N$, 但 $N_G(N) = G$, 矛盾. □

上述定理的证明 (本质上同 I, 例 7.11 的证明) 只应用了内交换群的可解性, 就变得十分简单. 但在 1952 年 Zassenhaus 第一次证明此定理时还很复杂, 尽管在 1903 年就已经知道了内交换群的构造.

应用 $\mathcal{P}$ 临界群来研究群性质 $\mathcal{P}$, 首先需要对 $\mathcal{P}$ 临界群的构造有尽可能多的了解, 最好是能把它们完全定出. 一般来说, $\mathcal{P}$ 临界群的构造相对于 $\mathcal{P}$ 群来说都是十分局限的. 下面的定理给出了内循环群的一个完全分类.

定理 6.7 设 G 是有限内循环群, 则 G 只有下列三种互不同构的类型:

(1) $G \cong Z_p \times Z_p$;

(2) G 为 8 阶四元数群;

(3) $G = \langle a, b \rangle$, 有如下的定义关系:

$$a^p = 1, b^{q^m} = 1, b^{-1}ab = a^r, \tag{6.1}$$

其中 p, q 为互异素数, m, r 为正整数, 且 $r \not\equiv 1 \pmod p$, $r^q \equiv 1 \pmod p$.

证　首先设 G 是交换群. 若 G 的所有 Sylow 子群皆循环, 则 G 本身循环. 因此由 G 是内循环群可推出对某个素数 p, G 必为 p- 群. 又由交换群分解定理 (I,4.7), 由 G 非循环推知 G 有 (p,p) 型子群 H. 但 G 为内循环群, 故必有 $G=H$, 即 $G\cong Z_p\times Z_p$ 为 (1) 型群.

再假定 G 非交换, 则 G 必为内交换群. 由定理 6.5, G 可解. 取 G 的极大正规子群 N, 则 N 循环, 且 $|G:N|=q$ 为素数. 我们先证明 $|G|$ 至多含有两个不同的素因子. 若否, 设 $q,p_1,\cdots,p_s$ 是 $|G|$ 的全部不同的素因子, $s\geq 2$, 则 N 必包含 G 的某个 Sylow p_i- 子群 P_i, $i=1,\cdots,s$. 并且因 P_i 是循环正规子群 N 的子群, 必有 $P_i\trianglelefteq G$. 再令 $Q\in \mathrm{Syl}_q(G)$. 则有 $\langle P_i,Q\rangle=P_iQ<G$, 于是 P_iQ 循环. 特别地, P_i 的生成元与 Q 的生成元可交换. 但因 $G=P_1\cdots P_s\cdot Q$, 则得 G 交换, 矛盾. 因此 G 至多含两个不同素因子. 下面分两种情形予以讨论.

(i) G 是 p- 群: 这时 G 有循环极大子群 N. 设 $N=\langle a_1\rangle$, $a_1^{p^n}=1$. 则由 G 非交换有 $n\geq 2$. 考虑商群 $G/\langle a_1^{p^2}\rangle=\overline{G}$. 易验证 $\overline{G}$ 仍为内循环群, 且 $|\overline{G}|=p^3$.(为证 G 非循环, 可用反证法, 这留给读者作为习题.) 根据 p^3 阶群的完全分类 (II,§3), 仅有的 p^3 阶内循环群为 8 阶四元数群, 故必有 $p=2$, 且 $G=\langle a_1,b\rangle$, 有关系

$$a_1^{2^n}=1,b^2=a_1^{2+4i},b^{-1}a_1b=a_1^{-1+4j},$$

其中 i,j 为适当的正整数. 令 $a=a_1^{1+2i}$, 则 a 仍为 N 的生成元. 以 a 代替 a_1, 则 $G=\langle a,b\rangle$, 有关系

$$a^{2^n}=1,b^2=a^2,b^{-1}ab=a^{-1+4j}.$$

因为

$$a^2=b^2=b^{-1}b^2b=b^{-1}a^2b=(b^{-1}ab)^2=a^{-2+8j},$$

得 $a^{4(1-2j)}=1$. 因 $1-2j$ 是奇数, 故得 $a^4=1$, 即 $n=2$. 于是 G 本身也必为四元数群, 即 G 为 (2) 型群.

(ii) G 不是 p- 群: 由前面的分析, 可设 $|G|=p^nq^m$, 且 G 的 Sylow p- 子群 $P\trianglelefteq G$, 但 G 的 Sylow q- 子群 $Q\ntrianglelefteq G$, P,Q 皆为循

环群. 于是可令 $G=\langle a,b\rangle$, 有关系

$$a^{p^n}=1, b^{q^m}=1, b^{-1}ab=a^r,$$

其中 r 为适当的正整数. 因 G 非交换, 故 $r\not\equiv 1 \pmod{p^n}$. 又因 b^q 与 a 生成 G 的真子群, 从而 b^q 与 a 可交换, 故 $r^q\equiv 1 \pmod{p^n}$. 同理, b 与 a^p 可交换, 又得 $a^p=b^{-1}a^pb=a^{rp}$, 于是 $r\equiv 1 \pmod{p^{n-1}}$. 这时我们断言必有 $n=1$, 因之 G 为 (3) 型群. 若否, 可令 $r=1+kp^{n-1}$, $(k,p)=1$. 于是有

$$r^q=(1+kp^{n-1})^q\equiv 1+kqp^{n-1} \pmod{p^n},$$

与 $r^q\equiv 1 \pmod{p^n}$ 矛盾.

反过来, 请读者自行验证 (1)–(3) 型群确为内循环群. 定理证毕. □

有了这个定理, 我们可以给第 II 章习题 28 的充分性部分一个十分简短的证明.

定理 6.8 设 G 是 n 阶群, $(n,\varphi(n))=1$. 则 G 循环.

证 因为 G 的任一子群的阶 m 是 n 的因子, 故亦有 $(m,\varphi(m))=1$, 于是定理的条件是子群遗传的. 若定理不真, 则其极小反例 G 为内循环群. 由条件 $(n,\varphi(n))=1$ 可推出 n 无平方因子, 于是 G 只能是定理 6.7 中的 (3) 型群, 且其中的 $m=1$. 因 G 非交换, 由 Sylow 定理, q 阶子群个数 $n_q=p$, 且 $p\equiv 1 \pmod q$, 故 $(n,\varphi(n))=(pq,(p-1)(q-1))=q\neq 1$, 矛盾. □

仿照这个定理的证明可得下面的十分有用的一般原则:

定理 6.9 设 $\mathcal{P}, \mathcal{P}_1$ 都是子群遗传的群性质, 且内 $\mathcal{P}$ 群均无性质 $\mathcal{P}_1$, 则 $\mathcal{P}_1$ 为 $\mathcal{P}$ 群的一个充分条件.

(证明从略).

类似的原则还有:

定理 6.10 设 $\mathcal{P}, \mathcal{P}_1$ 都是商群遗传的群性质，且外 $\mathcal{P}$ 群均无性质 $\mathcal{P}_1$，则 $\mathcal{P}_1$ 为 $\mathcal{P}$ 群的一个充分条件.

定理 6.11 设 $\mathcal{P}, \mathcal{P}_1$ 都是子群遗传并且商群遗传的群性质，且极小非 $\mathcal{P}$ 群均无性质 $\mathcal{P}_1$，则 $\mathcal{P}_1$ 为 $\mathcal{P}$ 群的一个充分条件.

这些原则说明了研究 $\mathcal{P}$ 临界群的重要性，它们在今后将要多次用到.

前面只举了内 $\mathcal{P}$ 群的例子，对于外 $\mathcal{P}$ 群的研究比较困难，故目前结果尚少. 即使是对外循环群和外交换群，也都有十分复杂的构造. 首先，它们都没有可解性. 事实上，任一非交换单群均为外循环群和外交换群. 因此，在研究外 $\mathcal{P}$ 群时，往往假定群的可解性，即只决定可解的外 $\mathcal{P}$ 群. 但即使如此，这方面的结果也不多，至于极小非 $\mathcal{P}$ 群，则往往是最容易确定的. 限于篇幅，也不在这里举例. 以后大家将会看到，所有这些 $\mathcal{P}$ 临界群的结果和方法在可解群和幂零群的理论中起着重要的作用.

在编写本节时，作者参考了陈重穆教授的下列文章：

1. 内 Σ 群，数学学报，**23**(1980), 239–243; **24**(1981), 331–335.

2. 内外超可解群与超可解群的充分条件，数学学报，**27**(1984), 694–703.

习　题

1–5 题是关于无限 Ω- 群的有限性条件的，读者也可先把它们略去.

1. 证明任一 Ω- 群关于 Ω- 子群的升链条件和极大条件等价，而降链条件和极小条件等价.

2. 抽象群 G 满足关于子群的极大条件的充要条件为 G 的每个子群都是有限生成的. 这个结论对于 Ω- 群成立吗？

3. 如果 Ω- 群 G 满足关于 Ω- 子群的极大 (或极小) 条件，则 G 的每个 Ω- 子群和 Ω- 商群也满足同一条件.

4. 设 N 是 Ω- 群 G 的正规 Ω- 子群，并且 N 和 G/N 都满足关于 Ω- 子群的极大 (或极小) 条件，则 G 也满足同一条件.

5. 设群 G 满足关于正规子群的极大条件. 若 $N \trianglelefteq G$, 且 $G \cong G/N$, 则 $N = 1$.

6. 设 H 是有限群 G 的 Hall 子群，且 $H \lhd \lhd G$, 则 $H \trianglelefteq G$.

7. 设 G 是有限群， $A \lhd \lhd G, B \lhd \lhd G$, 且 $(|A|, |B|) = 1$, 则 $\langle A, B\rangle = A \times B$.

8. 在上题中，用 A, B 无公共合成因子的条件去代替条件 $(|A|, |B|) = 1$, 结论仍然成立.

9. 举有限群的例子说明，群的合成群列并不一定都是由某个主群列加细而得来的.

10. 证明 A_5 的自同构群同构于 S_5.

11. 设群 G 只有两个合成因子，且都同构于 A_5, 则 $G \cong A_5 \times A_5$.

12. 设 V 是复数域 $\mathbb{C}$ 上 n 维向量空间，则 V 的加法群可以看成是以 $\mathbb{C}$ 为算子集合的算子群. 任一线性变换 μ 可看作 V 的 $\mathbb{C}$- 同态. 试用这个例子解释 Fitting 定理 (定理 2.6).

13. 接上题，设 λ 是 μ 的一个特征根，1 是 V 的恒等变换. 令 $\beta = \lambda \cdot 1 - \mu$, 则 β 亦为 V 的 $\mathbb{C}$- 自同态. 由 Fitting 定理，存在正整数 k 使

$$V = \mathrm{Ker}\ \beta^k \oplus V^{\beta^k}.$$

证明 Ker β^k 是 V 中对应于特征根 λ 的全体根向量组成的子空间，即属于 λ 的根子空间. 从而推出 V 可分解为属于 μ 的不同特征值的根子空间的直和.

14. 应用 13 题和 Krull-Schmidt 定理证明复数域上矩阵的 Jordan 标准型的分解定理.

15. 设 G 是有限 p- 群， $Z(G)$ 是循环群. 则 G 为不可分解群.

16. 决定所有的 pq 阶群，其中 $p \neq q$ 是素数.

17. 决定 $4p$ 阶群的不同构的类型，其中 p 是素数.

18. 定出所有阶 ≤ 30 的有限群 (16 阶和 24 阶群除外).

19. 证明不存在群 G 使 $G/Z(G)$ 同构于广义四元数群 Q_{4m}. 这里 $Q_{4m} = \langle x, y\rangle$, 有定义关系:

$$x^{2m} = 1, y^2 = x^m, y^{-1}xy = x^{-1}.$$

20. 在定理 4.3 中，设 H 是 N 的任一补群. 又设 $K \leq G$ 且 $(|K|, |N|) = 1$, 则存在 $n \in N$ 使 $n^{-1}Kn \leq H$.

21. 设 G 是群， 0 是一个符号， $0 \notin G$. 再设 n 是正整数，称元素在 $G \cup \{0\}$ 中的 n 级方阵为**单项矩阵**, 如果它的每行每列都恰有一个元素不为 0. 以 $M_n(G)$ 表所有 G 上 n 级单项矩阵的集合，并规定 0 与 G 中元素的加法、乘法运算如下:

$$0 \cdot x = x \cdot 0 = 0,\ 0 + x = x + 0 = x,\ \forall x \in G.$$

则 $M_n(G)$ 在通常矩阵乘法之下组成一个群，叫做 G 上的 n 级单项矩阵群. 证明

$$M_n(G) \cong G \wr S_n.$$

22. 设 G 是交换群. 对于 $A \in M_n(G)$, 规定 $\det A$ 为 A 中所有非 0 元素的乘积. 则映射

$$\alpha : A \mapsto \det A, \ \forall A \in M_n(G)$$

是 $M_n(G)$ 到 G 的满同态.

23. 设 G 是群， $H \leq G$, 且 $|G : H| = n$, $G = \bigcup_{i=1}^{n} Hg_i$ 是 G 对 H 的右陪集分解. 再没

$$P(x) = \begin{pmatrix} Hg_i \\ Hg_i x \end{pmatrix}, \ x \in G$$

是 G 在 H 上的置换表示. 规定

$$X = M(x) = (x_{ij}),$$

其中

$$x_{ij} = \begin{cases} g_i x g_j^{-1}, & \text{若} g_i x g_j^{-1} \in H, \\ 0, & \text{其它情形}, \end{cases}$$

则 $X \in M_n(H)$. 且映射

$$M : x \mapsto M(x) = X, \ x \in G$$

是 G 到 $M_n(H)$ 内的同构.

24. 试用单项矩阵及其行列式的概念给出转移映射 $V_{G\to H}$ 的新定义.

25. 设 G, H 都是抽象有限群. 以 $R(H)$ 表 H 的右正则表示，它是一个置换群. 记

$$G \wr_r H = G \wr R(H),$$

称为 G 和 H 的 正则圈积.

设 G, H, K 为三个有限群，均非平凡. 则正则圈积不成立结合律. 即一般没有

$$(G \wr_r H) \wr_r K = G \wr_r (H \wr_r K).$$

26. 设 G 是群， H 是集合 Ω 上的置换群，且 $G_1 \leq G, H_1 \leq H$. 则存在 $G_1 \wr H_1$ 到 $G \wr H$ 内的单同态. 如果 H 是抽象有限群，则也存在正则圈积 $G_1 \wr_r H_1$ 到 $G \wr_r H$ 内的单同态.

27. 设 G 是有限群，H 是有限集合 Ω 上的置换群. 又设 $G_p \in \mathrm{Syl}_p(G)$, $H_p \in \mathrm{Syl}_p(H)$. 则 $G_p \wr H_p \in \mathrm{Syl}_p(G \wr H)$.

28. 写出对称群 S_{27} 的 Sylow 3- 子群 P 的生成元.

29. 接上题, 证明 P 可由三个 3 阶元素生成, 但 P 中存在 27 阶元素.

30. 试决定所有的极小非循环群.

第 IV 章

幂零群和 p- 群

本章叙述有限幂零群和 p- 群的基本理论.

§1. 换位子

设 G 是群, 在第 I 章 §4 中定义了 G 中元素 a,b 的换位子 $[a,b]$, 本节将较详细地研究换位子的性质.

定义 1.1 设 G 是群, $a_1,\cdots,a_n\in G$, $n\geq 2$. 我们如下递归地定义 $a_1,\cdots,a_n$ 的**简单换位子** $[a_1,a_2,\cdots,a_n]$: 当 $n=2$ 时,

$$[a_1,a_2]=a_1^{-1}a_2^{-1}a_1a_2;$$

而当 $n>2$,

$$[a_1,a_2,\cdots,a_n]=[[a_1,a_2,\cdots,a_{n-1}],a_n].$$

下面是常用的换位子公式.

命题 1.2 设 G 是群, $a,b,c\in G$, 则

(1) $a^b=a[a,b]$;

(2) $[a,b]^c=[a^c,b^c]$;

(3) $[a,b]^{-1}=[b,a]=[a,b^{-1}]^b=[a^{-1},b]^a$;

(4) $[ab,c]=[a,c]^b[b,c]=[a,c][a,c,b][b,c]$;

(5) $[a,bc]=[a,c][a,b]^c=[a,c][a,b][a,b,c]$;

(6) (Witt 公式) $[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a=1$;

(7) $[a,b,c^a][c,a,b^c][b,c,a^b]=1$.

证 (1)–(3) 由定义直接验证.

(4) $[ab,c]=(ab)^{-1}c^{-1}abc=(c^{-1})^{ab}c=(a^{-1}c^{-1}a)^b c^b(c^{-1})^b c=(a^{-1}c^{-1}ac)^b[b,c]=[a,c]^b[b,c]=[a,c][a,c,b][b,c]$.

(5) $[a,bc]=[bc,a]^{-1}=([b,a]^c[c,a])^{-1}=[a,c][a,b]^c=[a,c][a,b]\cdot[a,b,c]$.

(6) 令 $u=aca^{-1}ba$. 轮换 a,b,c 三字母, 又令 $v=bab^{-1}cb$, $w=cbc^{-1}ac$. 则有

$$\begin{aligned}[a,b^{-1},c]^b &= b^{-1}[a,b^{-1}]^{-1}c^{-1}[a,b^{-1}]cb\\ &= b^{-1}ba^{-1}b^{-1}ac^{-1}a^{-1}bab^{-1}cb\\ &= (aca^{-1}ba)^{-1}(bab^{-1}cb)=u^{-1}v.\end{aligned}$$

同理有

$$[b,c^{-1},a]^c=v^{-1}w,\qquad [c,a^{-1},b]^a=w^{-1}u.$$

于是

$$[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a=u^{-1}vv^{-1}ww^{-1}u=1.$$

(7) 首先有

$$[a,b^{-1},c]^b=[[a,b^{-1}]^b,c^b]=[b,a,c^b].$$

同理又有

$$[b,c^{-1},a]^c=[c,b,a^c],\qquad [c,a^{-1},b]^a=[a,c,b^a],$$

于是由 Witt 公式有

$$[b,a,c^b][c,b,a^c][a,c,b^a]=1.$$

再互换 a,b 两个字母即得 (7) 式. □

定义 1.3 设 G 是群，A, B 是 G 的子群，则规定 A, B 的换位子群

$$[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle.$$

若 $A_1, \cdots, A_n$ 都是 G 的子群，$n > 2$, 同样规定

$$[A_1, \cdots, A_n] = \langle [a_1, \cdots, a_n] \mid a_i \in A_i \rangle.$$

命题 1.4 设 $A, B \le G$, 则

(1) $[A, B] = [B, A]$;

(2) $[A, B] \trianglelefteq \langle A, B \rangle$;

(3) 若 $A_1 \le A$, $B_1 \le B$, 则 $[A_1, B_1] \le [A, B]$;

(4) $[A, B]^\mu = [A^\mu, B^\mu]$, 其中 $\mu \in \mathrm{End}(G)$;

(5) $[A, B] \le A \iff B \le N_G(A)$;

(6) 若 A, B 都是 G 的正规 (或特征，或全不变) 子群，则 $[A, B]$ 亦然，并且 $[A, B] \le A \cap B$.

证 (1) 设 $a \in A, b \in B$. 因为 $[a, b] = [b, a]^{-1} \in [B, A]$, 得 $[A, B] \le [B, A]$. 类似的有 $[B, A] \le [A, B]$. 于是得 $[A, B] = [B, A]$.

(2) 设 $a, a_1 \in A, b, b_1 \in B$. 则由命题 1.2 中 (4), (5) 两式有

$$\begin{aligned} [a, b]^{b_1} &= [a, b_1]^{-1}[a, bb_1] \in [A, B], \\ [a, b]^{a_1} &= [aa_1, b][a_1, b]^{-1} \in [A, B], \end{aligned}$$

于是得 $[A, B] \trianglelefteq \langle A, B \rangle$.

(3) 显然.

(4) 由 $[a, b]^\mu = [a^\mu, b^\mu]$, $\mu \in \mathrm{End}(G)$, 立得结论.

(5) 由 $[a, b] = a^{-1}b^{-1}ab \in A \iff b^{-1}ab \in A$ 立得 $[A, B] \le A \iff b^{-1}Ab \subseteq A$, $\forall b \in B \iff B \le N_G(A)$.

(6) 由 (4) 立得前一结论；而由 (5), 因 A, B 正规，即得 $A, B \le A \cap B$. □

命题 1.5 (P. Hall 三子群引理) 设 A, B, C 是群 G 的子群，$N \trianglelefteq G$. 若 $[B, C, A] \le N$, $[C, A, B] \le N$, 则 $[A, B, C] \le N$.

证 对任意的 $a \in A, b \in B, c \in C$, 由 Witt 恒等式 (命题 1.2(6)) 得

$$[a, b^{-1}, c]^b = [c, a^{-1}, b]^{-a}[b, c^{-1}, a]^{-c}.$$

因为 $N \trianglelefteq G$, $[B, C, A] \leq N$, $[C, A, B] \leq N$, 上式右端属于 N, 于是得 $[a, b^{-1}, c]^b \in N$, 从而 $[a, b^{-1}, c] \in N$. 以 b^{-1} 代替 b, 即得 $[a, b, c] \in N$, 所以 $[A, B, C] \leq N$. □

注意，和定义 1.3 不同，有人把 $[A, B, C]$ 规定作 $[[A, B], C]$, 这时三子群引理依然成立，请读者仿照下面的命题 1.7 的证明方法自行证明.

定义 1.6 设 G 是群， n 是正整数. 如下定义子群 G_n: 规定 $G_1 = G$; 而当 $n > 1$ 时，规定 $G_n = \underbrace{[G, G, \cdots, G]}_{n个}$.

因为 $[g_1, g_2, \cdots, g_n] = [[g_1, g_2], g_3, \cdots, g_n] \in G_{n-1}$, 所以有 $G_n \leq G_{n-1}$. 又，明显地， G_n 是 G 的全不变子群.

我们称群列

$$G = G_1 \geq G_2 \geq G_3 \geq \cdots \geq G_n \geq \cdots$$

为群 G 的*下中心群列*.

命题 1.7 设 n 是正整数，则 $[G_n, G] = G_{n+1}$.

证 因为 $[g_1, \cdots, g_n, g_{n+1}] = [[g_1, \cdots, g_n], g_{n+1}]$, 有 $G_{n+1} \leq [G_n, G]$. 为证明 $[G_n, G] \leq G_{n+1}$, 我们先证明 $[[g_1, \cdots, g_n]^{-1}, g_{n+1}] \in G_{n+1}$. 由 1.2(3), 有 $[a^{-1}, b] = [a, b]^{-a^{-1}}$, 因此,

$$[[g_1, \cdots, g_n]^{-1}, g_{n+1}] = [g_1, \cdots, g_n, g_{n+1}]^{-[g_1, \cdots, g_n]^{-1}} \in G_{n+1}.$$

由定义， G_{n+1} 可由 $[c_1 c_2 \cdots c_s, g_{n+1}]$ 形状的元素生成，其中 $c_i = [g_1, \cdots, g_n]$ 或 $[g_1, \cdots, g_n]^{-1}$. 我们用对 s 的归纳法证明

$$[c_1 c_2 \cdots c_s, g_{n+1}] \in G_{n+1}.$$

因 $s=1$ 的情形已证，故设 $s>1$. 由 1.2(4),

$$[c_1c_2\cdots c_s, g_{n+1}] = [c_1c_2\cdots c_{s-1}, g_{n+1}]^{c_s}[c_s, g_{n+1}],$$

注意到 $G_{n+1} \trianglelefteq G$, 用归纳假设即得 $[c_1c_2\cdots c_s, g_{n+1}] \in G_{n+1}$. 于是 $G_{n+1} = [G_n, G]$. □

定理 1.8 设 G 是群, $G = \langle M \rangle$, 则

(1) $G_n = \langle [x_1, \cdots, x_n]^g \mid x_i \in M, g \in G \rangle$;

(2) $G_n = \langle [x_1, \cdots, x_n], G_{n+1} \mid x_i \in M \rangle$;

特别地有，若 $G = \langle a, b \rangle$, 则

(3) $G_2 = G' = \langle [a,b]^g \mid g \in G \rangle$;

(4) $G_2 = G' = \langle [a,b], G_3 \rangle$, 于是 G'/G_3 循环.

证 (1) 显然有 $[x_1, \cdots, x_n] \in G_n$. 若 $n=1$, 有 $G_1 = G = \langle M \rangle$, 结论成立. 设 $n>1$, 用对 n 的归纳法，可假设

$$G_{n-1} = \langle [x_1, \cdots, x_{n-1}]^g \mid x_i \in M, g \in G \rangle.$$

令

$$H = \langle [x_1, \cdots, x_n]^g \mid x_i \in M, g \in G \rangle.$$

显然 $H \trianglelefteq G$. 又因为对任意的 $g \in G$, 也有 $G = \langle M^g \rangle$, 于是由

$$[[x_1, \cdots, x_{n-1}]^g, x_n^g] = [x_1, \cdots, x_n]^g \in H,$$

知 G_{n-1} 的任一生成元 $[x_1, \cdots, x_{n-1}]^g$ 与 G 的每个生成元的换位子都在 H 中，于是 $G_n = [G_{n-1}, G] \leq H$. 而 $H \leq G_n$ 是明显的.

(2) 注意到

$$[x_1, \cdots, x_n]^g = [x_1, \cdots, x_n][x_1, \cdots, x_n, g],$$

由 (1) 立得 (2).

(3) 取 $M = \{a, b\}$, 注意到 $[b,a] = [a,b]^{-1}$, 由 (1) 得 (3).

(4) 因 $[a,b]^g = [a,b][a,b,g]$, 由 (3) 得 (4). □

§2. 幂零群

定义 2.1 称群列

$$G = K_1 \geq K_2 \geq \cdots \geq K_{s+1} = 1$$

为 G 的 *中心群列*, 如果 $[K_i, G] \leq K_{i+1}$, $i = 1, \cdots, s$. 这时称 s 为这个中心群列的长度. 由命题 1.4(5), 中心群列的任一项 $K_i \trianglelefteq G$, 且 $K_i/K_{i+1} \leq Z(G/K_{i+1})$.

存在中心群列的群叫做 *幂零群*.

定义 2.2 设 G 是群, 称群列

$$1 = Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_n(G) \leq \cdots$$

为 G 的 *上中心群列*, 如果对任意的 n, Z_n/Z_{n-1} 是 G/Z_{n-1} 的中心.

引理 2.3 设 G 是幂零群,

$$G = K_1 \geq K_2 \geq \cdots \geq K_{s+1} = 1$$

是 G 的一个中心群列. 则

(1) $K_i \geq G_i$, $i = 1, \cdots, s+1$;

(2) $K_{s+1-j} \leq Z_j(G)$, $j = 0, \cdots, s$.

证 (1) 用对 i 的归纳法. 当 $i = 1$ 时, $K_1 = G = G_1$, 结论成立. 下面设 $i > 1$, 且 $K_{i-1} \geq G_{i-1}$. 因为 $G_i = [G_{i-1}, G] \leq [K_{i-1}, G]$, 而 $K_{i-1}/K_i \leq Z(G/K_i)$, 有 $[K_{i-1}, G] \leq K_i$, 得证.

(2) 用对 j 的归纳法. 当 $j = 0$ 时, $K_{s+1} = 1 = Z_0(G)$, 结论成立. 下面设 $j > 0$, 且 $K_{s+1-(j-1)} \leq Z_{j-1}(G)$, 要证明 $K_{s+1-j} \leq Z_j(G)$. 而这等价于 $[K_{s+1-j}, G] \leq Z_{j-1}(G)$. 由 $[K_{s+1-j}, G] \leq K_{s+1-(j-1)}$ 即得所需结果. □

定理 2.4 设 G 是幂零群，则 G 的下中心群列终止于 1, 上中心群列终止于 G. 且它们都是定义 2.1 意义下的中心群列，并且二者的长度相同，记作 $c=c(G)$, 叫做 G 的幂零类. G 中不存在长度小于 c 的中心群列.

证　因为 G 幂零，存在中心群列

$$G=K_1 \geq K_2 \geq \cdots \geq K_{s+1}=1.$$

由引理 2.3 有 $K_i \geq G_i$, $K_{s+1-j} \leq Z_j(G)$. 取 $i=s+1$, $j=s$ 就推出 $G_{s+1}=1$, $Z_s(G)=G$. 这说明下中心群列终止于 1, 上中心群列终止于 G, 并且二者的长度都 $\leq s$. 由 $[G_i,G]=G_{i+1}$, $i=1,2,\cdots$ 推知下中心群列是中心群列；又由定义，上中心群列显然也是中心群列.

最后由引理 2.3, 因为上、下中心群列都是 G 的最短的中心群列，它们的长度必然相等. □

定理 2.5 (1) 若 G 是幂零群，$H \leq G, N \trianglelefteq G$, 则 H 和 $\overline{G}=G/N$ 亦幂零；

(2) 若 G_1, G_2 是幂零群，则 $G_1 \times G_2$ 亦幂零.

证　(1) 设

$$G=K_1 \geq K_2 \geq \cdots \geq K_{s+1}=1$$

是 G 的一个中心群列. 易验证

$$H=K_1 \cap H \geq K_2 \cap H \geq \cdots \geq K_{s+1} \cap H=1$$

和

$$\overline{G}=K_1N/N \geq K_2N/N \geq \cdots \geq K_{s+1}N/N=1$$

分别是 H 和 $\overline{G}$ 的中心群列，故 H 和 $\overline{G}$ 亦幂零.

(2) 由 $Z(G_1 \times G_2)=Z(G_1) \times Z(G_2)$ 及 G_1, G_2 的上中心群列分别终止于 G_1, G_2, 易推出 $G_1 \times G_2$ 的上中心群列终止于 $G_1 \times G_2$, 故得所需之结论. □

定理 2.6 有限 p- 群是幂零群.

证 由有限 p- 群 G 的中心 $Z(G)>1$ 及 $|G|$ 有限, 推知上中心群列必终止于 G, 于是 G 幂零. □

定理 2.7 设 G 是有限群, 则下述事项等价:

(1) G 是幂零群;

(2) 若 $H<G$, 则 $H<N_G(H)$;

(3) G 的每个极大子群 $M \trianglelefteq G$(这时 $|G:M|$ 为素数);

(4) G 的每个 Sylow 子群都是正规的, 因而 G 是它的诸 Sylow 子群的直积.

证 (1) $\Longrightarrow$ (2): 设 $H<G$, 则存在正整数 i 使 $H \geq G_{i+1}$, 但 $H \ngeq G_i$. 显然 $N_{G/G_{i+1}}(H/G_{i+1}) \geq G_i/G_{i+1}$, 于是 $N_G(H)/G_{i+1} \geq G_i/G_{i+1}$, $N_G(H) \geq G_i$. 这就推出必有 $N_G(H)>H$.

(2) $\Longrightarrow$ (3): 设 M 是 G 的极大子群, 由 (2), $M \trianglelefteq G$. 考虑 $\overline{G}=G/M$. 由 M 的极大性, $\overline{G}$ 没有非平凡子群, 故 $|\overline{G}|=|G:M|$ 是素数.

(3) $\Longrightarrow$ (4): 设 P 是 G 的 Sylow p- 子群, $H=N_G(P)$, 若 $G \neq H$, 取 G 的极大子群 $M>H$. 由 (3) 得 $M \trianglelefteq G$, 但由 II,2.5, $N_G(M)=M$, 矛盾. 故必有 $G=N_G(P)$, 即 $P \trianglelefteq G$. 于是 G 是它的诸 Sylow 子群的直积.

(4) $\Longrightarrow$ (1): 由定理 2.6 和定理 2.5(2) 立得. □

定理 2.8 幂零群 G 必为可解群.

证 容易用归纳法证明对任意正整数 i 有 $G_i \geq G^{(i-1)}$, 于是由 $G_{s+1}=1$ 可得到 $G^{(s)}=1$. 这样 G 是可解群. □

定理 2.9 设 G 幂零, $1 \neq N \trianglelefteq G$. 则 $[N,G]<N$, 且 $N \cap Z(G)>1$. 特别地, G 的每个极小正规子群含于中心 $Z(G)$ 之中.

证 令 $N_1=N$, 并对 $i>1$, 递归地定义 $N_i=[N_{i-1},G]$. 显然有 $N_i \leq N$, 并且 $N_i \leq G_i$. 由 G 幂零, 存在整数 c 使 $G_{c+1}=1$,

于是 $N_{c+1} = 1$. 这就推出 $N_2 = [N, G] < G$. (若否, 将推出对任意的 i, $N_i = N$, 矛盾.) 又, 设 t 满足 $N_t = 1$, 但 $N_{t-1} \neq 1$. 则由 $[N_{t-1}, G] = N_t = 1$ 知 $N_{t-1} \leq Z(G)$. 又有 $N_{t-1} \leq N$, 故 $N \cap Z(G) \geq N_{t-1} \neq 1$. □

定理 2.10 (P. Hall)

(1) 设

$$G = K_1 \geq K_2 \geq \cdots \geq K_{s+1} = 1 \tag{2.1}$$

是幂零群 G 的任一中心群列, 则对任意的 i, j 有 $[K_i, G_j] \leq K_{i+j}$.

(2) 对任意的 i, j 有 $[G_i, G_j] \leq G_{i+j}$, $[G_i, Z_j] \leq Z_{j-i}(G)$. 当 $j < i$ 时, 规定 $Z_{j-i}(G) = 1$. 特别地, 对任意的 i 都有 $[G_i, Z_i(G)] = 1$.

证 (1) 用对 j 的归纳法. 当 $j = 1$ 时, 由 (2.1) 式是中心群列, 有 $[K_i, G_1] = [K_i, G] \leq K_{i+1}$, 结论成立. 下面设 $j > 1$. 因 $G_j = [G_{j-1}, G]$, 有

$$[K_i, G_j] = [G_j, K_i] = [G_{j-1}, G, K_i].$$

又由归纳假设,

$$\begin{aligned} [G, K_i, G_{j-1}] &= [K_i, G, G_{j-1}] \leq [K_{i+1}, G_{j-1}] \\ &\leq K_{i+1+j-1} = K_{i+j}, \\ [K_i, G_{j-1}, G] &\leq [K_{i+j-1}, G] \leq K_{i+j}, \end{aligned}$$

于是由三子群引理 (命题 1.5), 有 $[G_{j-1}, G, K_i] \leq K_{i+j}$, 即 $[K_i, G_j] \leq K_{i+j}$.

(2) 分别以下中心群列和上中心群列代替 (1) 中的群列 (2.1), 即得结论. □

设 G 是可解群, 称满足 $G^{(r)} = 1$ 的最小的正整数 $r = r(G)$ 为 G 的 导列长. 这时 G 的导群列为

$$G = G^{(0)} > G^{(1)} > \cdots > G^{(r)} = 1.$$

下面的定理揭示了幂零群的导列长和幂零类之间的联系.

定理 2.11 设 G 是幂零群，则 $G^{(i)} \le G_{2^i}$, $i = 0, 1, \cdots, r$. 由此有 $r(G) \le \lceil \log_2(c+1) \rceil$, 其中 $\lceil a \rceil$ 表示不小于实数 a 的最小整数.

证 对 i 用归纳法. 当 $i = 0$ 时，结论显然成立. 设 $i > 0$, 因为

$$G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \le [G_{2^{i-1}}, G_{2^{i-1}}],$$

由 2.10(2), 即得 $G^{(i)} \le G_{2^{i-1}+2^{i-1}} = G_{2^i}$.

定理的第二部分请读者自证. □

§3. Frattini 子群

定义 3.1 设 G 是有限群. 若 $G \neq 1$, 令 $\Phi(G)$ 为 G 的所有极大子群的交；而若 $G = 1$, 令 $\Phi(G) = 1$. 我们称 $\Phi(G)$ 为 G 的 Frattini 子群或 G 的 Φ 子群.

显然有 $\Phi(G)$ char G.

为了研究 Frattini 子群进一步的性质，我们引进下面的概念.

定义 3.2 称 $x \in G$ 为群 G 的 **非生成元**, 如果由 $G = \langle S, x \rangle$ 可推出 $G = \langle S \rangle$, 这里 S 是 G 的一个子集.

例如， 1 是任意群的非生成元.

定理 3.3 群 G 的 Frattini 子群恰由 G 的所有非生成元组成.

证 设 $x \in \Phi(G)$, 并且 $G = \langle S, x \rangle$. 假定有 $\langle S \rangle < G$, 我们可取 G 的极大子群 $M \ge \langle S \rangle$. 由 $\Phi(G)$ 的定义有 $M \ge \Phi(G)$. 又因 $x \in \Phi(G)$, 有 $M \ge \langle S, x \rangle$, 与 $G = \langle S, x \rangle$ 矛盾. 故 x 是 G 的非生成元.

反之，设 x 是 G 的非生成元， M 是 G 的任一极大子群. 假定 $x \notin M$, 则 $\langle M, x \rangle = G$. 但 $\langle M \rangle = M \neq G$, 与 x 是 G 的非生成元相矛盾. 因此必有 $x \in M$. 由 M 的任意性，有 $x \in \Phi(G)$. □

定理 3.4 设 G 是有限群, $N \trianglelefteq G, H \le G$. 若 $N \le \Phi(H)$, 则 $N \le \Phi(G)$.

证 若 $N \not\le \Phi(G)$, 则有 G 的极大子群 M 使 $N \not\le M$, 且由 M 的极大性, 有 $G = NM$. 这时 $H = H \cap NM = N(H \cap M)$. 因为 $N \le \Phi(H)$, 由定理 3.3 有 $H = H \cap M$, 即 $H \le M$, 当然也有 $N \le M$, 矛盾. □

推论 3.5 设 G 是有限群, $K \trianglelefteq G$. 则 $\Phi(K) \le \Phi(G)$.

证 由 $K \trianglelefteq G$, $\Phi(K)$ char K, 有 $\Phi(K) \trianglelefteq G$, 在上定理中取 $N = \Phi(K)$, $H = K$, 即得所需之结论. □

注 3.6 若 G 是有限群, $K \le G$, 一般不能推出 $\Phi(K) \le \Phi(G)$, 请读者举例说明之.

定理 3.7 (Gaschütz) 设 G 是有限群, N, D 是 G 的正规子群, 且 $D \le N$, $D \le \Phi(G)$. 若 N/D 幂零, 则 N 本身亦幂零.

证 设 P 是 N 的 Sylow p- 子群, 则 PD/D 是 N/D 的 Sylow p- 子群. 由 N/D 幂零, PD/D char N/D. 于是 $PD/D \trianglelefteq G/D$, 这得到 $PD \trianglelefteq G$. 由 Frattini 论断有 $PDN_G(P) = G$. 又由 $D \le \Phi(G)$, 据定理 3.3, 有 $G = PN_G(P) = N_G(P)$, 所以 $P \trianglelefteq G$, 自然也有 $P \trianglelefteq N$. 由 p 的任意性, N 的任一 Sylow 子群均系正规子群, 从而 N 幂零. □

推论 3.8 (Frattini 定理) 有限群 G 的 Frattini 子群 $\Phi(G)$ 必幂零.

证 在 3.7 中令 $N = D = \Phi(G)$, 即得结论. □

推论 3.9 若 $G/\Phi(G)$ 幂零, 则 G 本身幂零.

证 在 3.7 中令 $N = G$, $D = \Phi(G)$, 即得结论. □

定理 3.10 若素数 $p \mid |\Phi(G)|$, 则 $p \mid |G/\Phi(G)|$.

证 假定 $p \nmid |G/\Phi(G)|$, 设 P 是 $\Phi(G)$ 的 Sylow p- 子群，则 P 也是 G 的 Sylow p- 子群. 由 3.8, $\Phi(G)$ 幂零，于是 P char $\Phi(G)$, $P \trianglelefteq G$. 因 $(|G/P|, |P|) = 1$, 由 Schur-Zassenhaus 定理， P 在 G 中有补 H, 于是 $G = HP$. 又因 $P \leq \Phi(G)$, 得 $G = H$, 矛盾. □

定理 3.11 (Wielandt) *有限群 G 幂零当且仅当 $G' \leq \Phi(G)$.*

证 若 $G' \leq \Phi(G)$, 则 $G/\Phi(G)$ 交换，因而也幂零. 由推论 3.9, G 幂零. 反之，若 G 幂零，则 G 的任一极大子群 M 的指数 $|G : M| = p$. 于是 G/M 交换，所以 $G' \leq M$. 由 M 的任意性有 $G' \leq \Phi(G)$. □

§4. 内幂零群

在第 III 章 §6, 我们对 $\mathcal{P}$ 临界群作了初步讨论，本节我们来研究内幂零群. 首先我们有下面的

定理 4.1 (Schmidt) *设 G 是内幂零群，则 G 可解.*

证 设 G 是一最小阶反例. 明显地，由 G 的每个真子群幂零, 可推出 G 的每个同态像的真子群也幂零. 因此, 若有 $1 \neq N \lhd G$, 则由 N 幂零， G/N 可解，可得 G 可解. 于是最小阶反例 G 只能是非交换单群.

设 M_1, M_2 是 G 的两个不同的极大子群，使 $D = M_1 \cap M_2$ 的阶最大.

假定 $D \neq 1$, 则由 M_i 的幂零性，有

$$1 < D < N_{M_i}(D) = H_i, \ i = 1, 2.$$

于是 $D \trianglelefteq H_i \leq M_i$, $i = 1, 2$, 又由 G 是单群， $N_G(D) < G$, 必存在 G 的极大子群 $M_3 \geq N_G(D)$. 这时由 $D < H_1 \leq M_1 \cap M_3$ 以及 D 的最大性得 $M_1 = M_3$. 同理可得 $M_2 = M_3$. 这样 $M_1 = M_2$, 矛盾.

因此 G 的任二极大子群之交必为 1. 设 M 是 G 的一个极大子群, 由 G 是单群, 有 $N_G(M) = M$. 于是 M 在 G 中恰有 $|G : M|$

个共轭子群. 考虑 G 的所有极大子群, 设它们共有 s 个共轭类, 而 $M_1,\cdots,M_s$ 是在每个共轭类中取出的代表. 这时有

$$\begin{aligned}|G| &= 1+\sum_{i=1}^{s}(|M_i|-1)|G:M_i| \\ &= 1+s|G|-\sum_{i=1}^{s}|G:M_i|.\end{aligned}$$

由 $|G:M_i|\le\frac{|G|}{2}$, 推出

$$|G|\ge 1+s|G|-\frac{s|G|}{2}=1+\frac{s|G|}{2},$$

因此必有 $s=1$. 但这时又有

$$|G|=1+|G|-|G:M_1|,$$

推出 $G=M_1$, 矛盾. 于是 G 是可解的. □

定理 4.2 设 G 是内幂零群, 则 G 有下列性质:

(1) $|G|=p^aq^b$, $p\ne q$ 均为素数, 且适当选择符号使有 G 的 Sylow p- 子群 $P\trianglelefteq G$, 而 Sylow q- 子群 Q 循环, 故 $Q\ntrianglelefteq G$, 并有 $\Phi(Q)\le Z(G)$;

(2) $\Phi(P)\le Z(G)$. 特别地 $c(P)\le 2$;

(3) 若 $p>2$, 则 $\exp P=p$; 而若 $p=2$, 则 $\exp P\le 4$.

证 (1) 由定理 4.1, G 是可解的. 设 $|G|=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$. 因为 p- 群是幂零的, 有 $r>1$. 由 G 可解, 存在 G 的极大子群 $M\trianglelefteq G$, 且 $|G:M|$ 是素数, 譬如 $|G:M|=p_1$. 由 M 幂零, 对于任意的 i, M 的 Sylow p_i- 子群 P_i 在 M 中正规. 而对 $i>1$, M 的 Sylow p_i- 子群 P_i 也是 G 的 Sylow p_i- 子群, 于是 $P_i\trianglelefteq G$. 现在假定 $r\ge 3$, 设 P_1 是 G 的 Sylow p_1- 子群. 由 $P_1P_i<G$, 有 P_1P_i 幂零. 这样, 对 $i>1$, P_1 的元素和 P_i 的元素可交换, 于是亦有 $P_1\trianglelefteq G$. 这推出 $G=P_1\times P_2\times\cdots\times P_r$, G 幂零, 矛盾. 因此有 $r=2$.

设 $|G|=p^aq^b$. 前面已证 G 一定有正规 Sylow 子群, 不妨设 G 有正规 Sylow p- 子群 P. 又设 Q 是 G 的一个 Sylow q- 子群,

M 是 Q 的极大子群. 则由 $PM < G$ 知 PM 幂零, 于是 P 中元素与 M 中元素可交换. 若 Q 又有另一极大子群 M_1, 同法可得 P 中元素与 M_1 中元素交换. 因 $\langle M, M_1\rangle = Q$, 有 P 中元素与 Q 中元素交换, 从而 $Q \trianglelefteq G$, G 亦幂零, 矛盾. 所以 Q 只有唯一的极大子群, 这时 Q 是循环群. 它的唯一的极大子群是 $\Phi(Q)$, 并且有 $\Phi(Q) \leq Z(G)$.

(2) 首先证 Q 的正规闭包 $Q^G = G$. 若否, 有 $Q^G < G$, 则 Q^G 幂零. 因 Q 是 G 的而且也是 Q^G 的 Sylow q- 子群. 所以有 Q char Q^G. 由 $Q^G \trianglelefteq G$, 得 $Q \trianglelefteq G$, 矛盾.

现在设 N 是任一真含于 P 的 G 的正规子群. 我们要证明 $N \leq Z(G)$. 由于 $QN < G$, 故 QN 幂零, 于是 $N \leq C_G(Q)$, 又对任意的 $g \in G$, 有 $N = N^g \leq C_G(Q^g)$. 而 $Q^G = \langle Q^g \mid g \in G\rangle$, 故 $N \leq C_G(Q^G) = C_G(G) = Z(G)$.

因 $\Phi(P)$ char P, $P \trianglelefteq G$, 有 $\Phi(P) \trianglelefteq G$, 故 $\Phi(P)$ 是一真含于 P 的 G 正规子群, 于是有 $\Phi(P) \leq Z(G)$. 又由 P 幂零, 有

$$P' \leq \Phi(P) \leq P \cap Z(G) \leq Z(P),$$

这可得到 $c(P) \leq 2$.

(3) 首先, 由 $[P, Q] \trianglelefteq \langle P, Q\rangle = G$, 且 $[P, Q] \leq P$, 故 $[P, Q]$ 为含于 P 的 G 的正规子群. 若 $[P, Q] < P$, 由 (2) 的证明有 $[P, Q] \leq Z(G)$. 令 $\overline{G} = G/Z(G)$, 有 $[\overline{P}, \overline{Q}] = \overline{1}$, 于是 $\overline{G}$ 幂零, 从而 G 亦幂零, 矛盾. 故我们得到 $[P, Q] = P$, 即

$$P = \langle [x, y] = x^{-1}x^y \mid x \in P, y \in Q\rangle. \tag{4.1}$$

又因 $c(P) \leq 2$, 由第 I 章 §4 习题 10 (取 $n = p$) 有对任意的 $a, b \in P$,

$$[a, b]^p = [a^p, b], \quad (ab)^p = a^p b^p [b, a]^{\binom{p}{2}}. \tag{4.2}$$

由 $a^p \in \Phi(P) \leq Z(G)$, 有 $[a^p, b] = 1$, 故 $[a, b]^p = 1$. 若 $p \neq 2$, 则有

$$(ab)^p = a^p b^p,\ \forall a, b \in P. \tag{4.3}$$

现在对任意的 $x \in P, y \in Q$, 由 $x^p \in Z(G)$ 有 $[x^p, y] = 1$, 即 $x^{-p}y^{-1}x^p y = x^{-p}(x^y)^p = 1$. 由 (4.3) 式得 $(x^{-1}x^y)^p = 1$, 即 $[x, y]^p =$

1. 再由 (4.1) 式, P 可由若干 p 阶元素生成, 最后用 (4.3) 式, 即得到 $\exp P = p$.

对于 $p = 2$, 仍有

$$a^2 \in Z(G) \quad \text{和} \quad [a,b]^2 = 1,\ \forall a, b \in P.$$

由第 I 章 §4 习题 10 (取 $n = 4$), 有

$$(x^{-1}x^y)^4 = x^{-4}(x^y)^4[x^y, x^{-1}]^6 = 1,\ \forall x \in P, y \in Q,$$

和

$$(ab)^4 = a^4b^4[b,a]^6 = a^4b^4,\ \forall a, b \in P,$$

这就得到 $\exp P \le 4$. □

应用内幂零群的构造, 我们可得到幂零群的下述充分条件.

定理 4.3 (Itô) *设 $|G|$ 是奇数.*

(1) 若群 G 的每个极小子群都含于 $Z(G)$, 则 G 幂零;

(2) 若 G' 的每个极小子群都在 G 中正规, 则 G' 幂零, 而 G 可解.

证 (1) 设 G 是最小阶反例. 首先, 定理的条件显然在取子群下是遗传的. 于是 G 的每个真子群幂零, 但 G 不幂零. 由定理 4.2, 有 $G = PQ$, 其中 $P \trianglelefteq G$, Q 循环, 且 $\exp P = p$. 再由定理条件, P 中每个元素都属于 $Z(G)$, 于是 $P \le Z(G)$. 这样 $G = P \times Q$, G 幂零, 矛盾.

(2) 设 H 是 G' 的一个极小子群, 则 $|H| = p$ 是素数. 由 $H \trianglelefteq G$, 对 H 用 N/C 定理, 有 $G/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的子群, 因而是交换群. 这样有 $C_G(H) \ge G'$, 于是 $H \le Z(G')$, 由 (1) 得 G' 幂零, 又由 G/G' 交换, 得 G 可解. □

§5. p- 群的初等结果

从本节起, 我们继续研究有限 p- 群. 为了研究 p- 群的 Frattini 子群. 我们规定

$$\mho_1(G) = \langle g^p \mid g \in G \rangle.$$

(这和 I,4.7 证明中对交换 p- 群 A 规定 $\mho_1(A)$ 是一致的.) 显然 $\mho_1(G)$ char G, 且 $\exp(G/\mho_1(G)) = p$, 并有下面的

定理 5.1 *设 G 是有限 p- 群, 则 $\Phi(G) = G'\mho_1(G)$, 且 $G/\Phi(G)$ 是初等交换 p- 群. 并且若 $N \trianglelefteq G$, G/N 是初等交换 p- 群, 则 $\Phi(G) \le N$.*

证 设 $g \in G$, M 是 G 的任一极大子群, 则 $M \trianglelefteq G$, 且 G/M 是 p 阶循环群, 于是有 $g^p \in M$. 由 M 的任意性有 $g^p \in \Phi(G)$, 这样 $\mho_1(G) \le \Phi(G)$. 又由 G 幂零, 据定理 3.11 有 $G' \le \Phi(G)$, 于是 $G'\mho_1(G) \le \Phi(G)$.

下面设 $N \trianglelefteq G$, 且 G/N 是初等交换 p- 群, 我们来证明 $\Phi(G) \le N$. 设 $|G/N| = p^r$. 因为 G/N 作为初等交换 p- 群可以看作域 $GF(p)$ 上的 r 维向量空间, 显然可以找到 r 个 $r-1$ 维子空间, 使它们的交是零空间. 这就推出存在 G 的 r 个极大子群, 其交为 N. 由 Frattini 子群的定义就有 $\Phi(G) \le N$, 最后, 因为 $G/G'\mho_1(G)$ 是初等交换 p- 群, 有 $\Phi(G) \le G'\mho_1(G)$, 于是 $\Phi(G) = G'\mho_1(G)$. □

定理 5.2 (Burnside 基定理) *设 G 是有限 p- 群, $|G/\Phi(G)| = p^d$, 则 G 的每个最小生成系恰含 d 个元素. 并且每个 $G \setminus \Phi(G)$ 中的元素 x 都至少属于一个最小生成系.*

证 由定理 3.3, $G = \langle x_i \mid i \in I\rangle$ 当且仅当 $G/\Phi(G) = \langle x_i\Phi(G) \mid i \in I\rangle$, 由于 $G/\Phi(G)$ 可看成 $GF(p)$ 上 d 维向量空间, 故其最小生成系恰含 d 个元素, 于是对 G 也有同样的结论.

设 $x \in G \setminus \Phi(G)$, 则 $x\Phi(G)$ 在线性空间 $G/\Phi(G)$ 中不是零向量, 于是可扩充成 $G/\Phi(G)$ 的一组基 $x\Phi(G) = x_1\Phi(G), \cdots, x_d\Phi(G)$. 这时 $\{x_1, \cdots, x_d\}$ 就是 G 的一组最小生成系. □

由这个定理, 我们还得到有限 p- 群的一个重要的算术不变量 $d = d(G)$, 常称为 p- 群 G 的**秩**.

定理 5.3 (P. Hall) *设 $|G| = p^n$, 则*

$$|\mathrm{Aut}(G)| \mid p^{d(n-d)}(p^d - 1)(p^d - p)\cdots(p^d - p^{d-1}).$$

证 首先对任一 $\alpha \in \mathrm{Aut}(G)$, 可如下得到 $G/\Phi(G)$ 的一个自同构 $\bar{\alpha}$:

$$(g\Phi(G))^{\bar{\alpha}} = g^{\alpha}\Phi(G), \ \forall g \in G.$$

易验证 $f : \alpha \mapsto \bar{\alpha}$ 是 $\mathrm{Aut}(G)$ 到 $\mathrm{Aut}(G/\Phi(G))$ 上的同态，于是 $|(\mathrm{Aut}(G))^f|$ 整除 $|\mathrm{Aut}(G/\Phi(G))|$. 把 $G/\Phi(G)$ 看作 $GF(p)$ 上 d 维向量空间，则有

$$\begin{aligned} & |\mathrm{Aut}(G/\Phi(G))| = |GL(d,p)| \\ = \ & (p^d - 1)(p^d - p)\cdots(p^d - p^{d-1}). \end{aligned}$$

再令 $K = \mathrm{Ker}\, f$, 为研究 K 的阶，我们设 $\{x_1, \cdots, x_d\}$ 是 G 的任一最小生成系. 考察所有的有序 d 元子集 $\{x_1a_1, \cdots, x_da_d\}$ 组成的集合 Δ, 其中 $a_i \in \Phi(G)$. 显然 Δ 的每个元素都是 G 的最小生成系，并且 $|\Delta| = |\Phi(G)|^d = p^{(n-d)d}$. 令 K 作用在 Δ 上， Δ 被分成若干个 K 的轨道 $T_1, \cdots, T_s$. 每个 T_i 的长度 $|T_i| = |K|/|K_i|$, 其中 K_i 是由把 T_i 中某个最小生成系保持不变的 G 的自同构所组成的. 但明显地，这样的同构只能是 1, 于是 $K_i = 1$. 这样, $|T_i| = |K|$. 最后因 $|\mathrm{Aut}(G)| = |K||\mathrm{Aut}(G)^f|$, 即得所需之结论. □

在上述定理证明中出现的子群 $K = \mathrm{Ker}\, f$ 通常记作 $\mathrm{Aut}^{\Phi}(G)$, 它是由所有在 $G/\Phi(G)$ 上诱导出恒等自同构的 G 的自同构所组成. 上述定理的证明告诉我们，对于任意的有限 p- 群 G, $\mathrm{Aut}^{\Phi}(G)$ 也是 p- 群.

定理 5.4 *有限 p- 群 G 的每个合成因子和主因子皆为 p 阶循环群.*

证 因为 G 是可解的, 故 G 的每个合成因子为 p 阶循环群. 又因 G 是幂零的，由 G 的任一中心群列出发，把它加细成主群列，得到的主因子也必然都是 p 阶循环群 (这是因为含于中心的任一子群必为正规子群). 再由 Jordan-Hölder 定理即得任一主群列的主因子为 p 阶循环群. □

定理 5.5 有限 p- 群 G 的任一子群皆为次正规子群.

证 设 $H \le G$, $|G:H| = p^s$. 我们对 s 作归纳法. 若 $s = 1$, 则 $H \trianglelefteq G$, 定理成立, 现在假定 $s > 1$, 并设定理对 $< s$ 的情形已经成立, 因为 $H < G$, 有 $H < N_G(H) = H_1$. 这时有 $H \trianglelefteq H_1$, $|G:H_1| < p^s$, 由归纳假设, $H_1 \lhd \lhd G$. 再由次正规性可传递, 有 $H \lhd \lhd G$. □

推论 5.6 设 G 是有限 p- 群, $H_1 \le H_2$ 是 G 的子群 (正规子群), $|H_2 : H_1| = p^s$. 则对任意的非负整数 $t \le s$, 存在 G 的子群 (正规子群) H_3, 使 $H_1 \le H_3 \le H_2$, 且 $|H_3 : H_1| = p^t$.

证 对于子群的情形, 因为 $H_1 \lhd \lhd H_2$, $H_2 \lhd \lhd G$, 故存在 G 的次正规群列以 H_1, H_2 为其中两项. 把此群列加细成 G 的合成群列, 则满足条件的子群 H_3 的存在性就是明显的. 对于正规子群的情形, 只有把群列 $1 \le H_1 \le H_2 \le G$ 加细成 G 的主群列, 由定理 5.4, 也立即推出满足定理条件的正规子群 H_3 的存在性. □

下面的定理可以看作是 II, 定理 3.11 的推广.

定理 5.7 设 G 是有限 p- 群. 若 $N \trianglelefteq G$, $|N| = p^i$, 则 $N \le Z_i(G)$.

证 当 $i = 0$ 时, 结论是显然的. 而对 $i = 1$, 即定理 II,3.11, 故可设 $i > 1$. 取 $N_1 \trianglelefteq G$, 满足 $N_1 < N$ 且 $|N_1| = p^{i-1}$, 则由归纳假设有 $N_1 \le Z_{i-1}(G)$, 由

$$\overline{N} = NZ_{i-1}(G)/Z_{i-1}(G) \cong N/N \cap Z_{i-1}(G),$$

及 $N \cap Z_{i-1}(G) \ge N_1$, 得 $|\overline{N}| \le p$. 由定理 II,3.11, 有 $\overline{N} \le Z_i(G)/Z_{i-1}(G)$. 于是 $NZ_{i-1}(G) \le Z_i(G)$, $N \le Z_i(G)$. □

定理 5.8 设 G 是有限 p- 群.
(1) 若 $N \le Z(G)$, 且 G/N 循环, 则 G 交换;
(2) 若 G 不交换, 则 $d(G/Z(G)) \ge 2$. 特别地, $p^2 \mid |G/Z(G)|$;
(3) 若 G 不交换, 则 $d(G/G') \ge 2$. 特别地, $p^2 \mid |G/G'|$.

证 (1) 设 $G/N = \langle xN \rangle$, 则 $G = \langle x, N \rangle$. 因 $N \le Z(G)$, G 的生成元间彼此可交换，于是 G 是交换群.

(2) 由 (1) 立得.

(3) 因为 $G' \le \Phi(G)$, 若 $d(G/G') = 1$, 则 $d(G/\Phi(G)) = 1$, 于是 $d(G) = 1$, 与 G 不交换矛盾. □

引理 5.9 *设 N 是有限 p- 群 G 的非循环正规子群.*

(1) 若 $p > 2$, 则存在 G 的 (p,p) 型交换正规子群 $A \le N$;

(2) 若 $p = 2$, (1) 中结论一般不真. 但若有 $N \le \Phi(G)$, 则 (1) 中结论成立.

证 对 $|N|$ 用归纳法. 当 $|N| = p^2$, 则因 N 非循环，N 本身是 (p,p) 型交换群，引理成立.

现在设 $|N| \ge p^3$. 取 G 的 p 阶正规子群 $P < N$. 考虑商群 G/P, 它具有正规子群 N/P.

(i) 若 N/P 循环，则由定理 5.8(1), N 是交换群. 由 N 非循环，$\Omega_1(N) = \langle x \in N \mid x^p = 1 \rangle$ 必为 (p,p) 型交换群. 又由 $\Omega_1(N)$ char N, $N \trianglelefteq G$, 即得 $\Omega_1(N) \trianglelefteq G$, 引理成立.

(ii) 若 N/P 不循环，则由归纳假设，N/P 中存在 G/P 的 (p,p) 型交换正规子群 M/P. 这时 M 是 G 的 p^3 阶非循环正规子群. 如果 M 交换，则 $|\Omega_1(M)| \ge p^2$. 且 $\Omega_1(M) \trianglelefteq G$. 在 $\Omega_1(M)$ 中取出 G 的 p^2 阶正规子群即合要求. 如果 $\Omega_1(M)$ 不交换，再分别 $p > 2$ 和 $p = 2$ 两种情形:

(1) $p > 2$. 这时 M 可能有两种类型，即第 II 章 §3 中 (I) 型和 (II′) 型. 对于 (I) 型群，$\Omega_1(M) = \langle a^p, b \rangle$, 是 (p,p) 型交换群，并且有 $\Omega_1(M) \trianglelefteq G$. 而对于 (II′) 型群，任取包含在 M 中的 G 的 p^2 阶正规子群，都满足引理的要求.

(2) $p = 2$. 如果 $G = N = Q$, Q 是四元数群，则显然引理不真. 但若补充假定 $N \le \Phi(G)$, 则 $M \le \Phi(G)$. 如果 M 中没有 G 的 (2,2) 型正规子群，则必有 4 阶循环子群 $\langle x \rangle \trianglelefteq G$. 对 $\langle x \rangle$ 用 N/C 定理有 $G/C_G(x)$ 同构于 $\mathrm{Aut}(Z_4) \cong Z_2$ 的一个子群. 于是 $|G/C_G(x)| \le 2$. 这样 $C_G(x) \ge \Phi(G) \ge M$, 推出 M 是交换群，矛盾. □

定理 5.10 设 G 是有限 p- 群，且 G 的每个交换正规子群皆为循环群.

(1) 若 $p>2$, 则 G 本身是循环群;

(2) 若 $p=2$, 则 G 中有循环极大子群.

证 (1) 若 G 不循环，在引理 5.9 中取 $N=G$, 则 G 存在 (p,p) 型交换正规子群，与假设矛盾.

(2) 首先，在引理 5.9(2) 中取 $N=\Phi(G)$, 得 $\Phi(G)$ 循环. 再取 G 的极大交换正规子群 $A\geq\Phi(G)$, 由条件有 A 循环，并且因 $A\geq\Phi(G)$, 则 G/A 为初等交换 2- 群. 若 $|G/A|=2$, 则 A 为 G 的循环极大子群，定理得证. 故可设 $|G/A|>2$. 又由 A 的极大性，必有 $C_G(A)=A$. (若否，取 $x\in C_G(A)\setminus A$, 命 $B=\langle x,A\rangle$, 则有 B 交换且 $B>A$. 由 G/A 交换，有 $B\trianglelefteq G$, 与 A 的极大性矛盾.) 对 A 用 N/C 定理，有 $G/C_G(A)=G/A\lesssim \mathrm{Aut}(A)$. 我们假设 $A=\langle a\rangle$, $|A|=2^n$. 据第 I 章 §3 习题 2, 仅当 $n\geq3$ 时 $\mathrm{Aut}(A)$ 非循环，且这时有 $\mathrm{Aut}(A)\cong Z_2\times Z_{2^{n-2}}$. 故可令 $n\geq3$, 且 G/A 是 (2,2) 型交换群. 于是 $G/A\cong\Omega_1(\mathrm{Aut}(A))$, 因此 G 中元素依共轭作用可诱导出 A 的三个 2 阶自同构中的任何一个，特别地，必存在 $b\in G\setminus A$ 使得

$$a\mapsto b^{-1}ab=a^{1+2^{n-1}}.$$

因为 $b^2\in\langle a\rangle$, 可令 $b^2=a^r$. 若 r 为奇数，则 $\langle b\rangle>\langle a\rangle$, $\langle b\rangle$ 亦为 G 之循环正规子群，矛盾于 A 的选取. 故 r 必为偶数. 令 $r=2s$, 注意到 $n\geq3$, 于是存在整数 i 使同余式

$$i(1+2^{n-2})+s\equiv0\ (\mathrm{mod}\ 2^{n-1})$$

成立. 令 $b_1=ba^i$, 则

$$\begin{aligned}b_1^2=b^2(b^{-1}a^ib)a^i &= b^2a^{i(1+2^{n-1})+i}=a^ra^{2i(1+2^{n-2})}\\ &= a^{2s+2i(1+2^{n-2})}=1.\end{aligned}$$

于是 b_1 是 2 阶元， G 的极大子群 $M=\langle b_1,a\rangle$ 有定义关系:

$$a^{2^n}=1,\ b_1^2=1,\ b_1^{-1}ab_1=a^{1+2^{n-1}}.$$

由计算知，M 中 ≤ 2 阶的元素组成子群 $\Omega_1(M) = \langle b_1, a^{2^{n-1}} \rangle$. 显然 $\Omega_1(M)$ char M, 又 $M \trianglelefteq G$, 得 $\Omega_1(M) \trianglelefteq G$, 与 G 没有非循环交换正规子群矛盾. □

注 5.11 设 G 是有限 p- 群，通常我们规定

$$\delta = \delta(G) = \max\{d(A) \mid A \trianglelefteq G,\ A' = 1\},$$

并称 δ 为 G 的 深(depth). 定理 5.10(1) 对 $p > 2$ 的情形决定了 $\delta = 1$ 的有限 p- 群. Blackburn 在下文中对 $p > 2$ 的情形决定了所有 $\delta = 2$ 的有限 p- 群. 这个结果后来被 Feit 和 Thompson 成功地用在奇数阶群可解性的研究中.

N.Blackburn, Generalizations of certain elementary theorems on p-groups, *Proc. London Math. Soc.*, **11**(1961), 1–22.

定理 5.12 *设 G 是有限 p- 群.*

(1) 若 $G' \cap Z_2(G)$ 循环，则 G' 循环;

(2) 若 $Z(G')$ 循环，则 G' 循环;

(3) 若 $Z(\Phi(G))$ 循环，则 $\Phi(G)$ 循环.

证 (1) 若 G' 不循环，则由 $G' \le \Phi(G)$, 据引理 5.9, 存在 G 的 (p,p) 型正规子群 $A \le G'$. 由 $|A| = p^2$, 推知 $A \le Z_2(G)$. 于是 $A \le G' \cap Z_2(G)$, 与假设矛盾.

(2) 由 2.10(2), $[G', Z_2(G)] = 1$, 于是 $G' \cap Z_2(G) \le Z(G')$. 由 $Z(G')$ 循环，则 $G' \cap Z_2(G)$ 循环，由 (1) 即得结论.

(3) 设 $Z(\Phi(G))$ 循环，但 $\Phi(G)$ 不循环. 由引理 5.9, 存在 G 的 (p,p) 型正规子群 $A \le \Phi(G)$. 对 A 用 N/C 定理，有 $|G/C_G(A)|$ 是 $|\mathrm{Aut}(A)|$ 的因子. 但 $|\mathrm{Aut}(A)| = (p^2-1)(p^2-p)$, 这得到 $|G/C_G(A)| \le p$. 于是 $\Phi(G) \le C_G(A)$, 即 $A \le Z(\Phi(G))$, 矛盾. □

注 5.13 W. Burnside 早在本世纪初就研究过这样的问题：究竟什么样的群可以作为一个有限 p- 群的导群？定理 5.12(2) 就是他证明的结果. 它说明一个中心循环的非循环 p- 群不能作为任何一个有限 p- 群的导群. 另外一个与此类似的问题是：什么样的群可

以作为一个有限 p- 群的 Φ 子群？定理 5.12(3) 对这个问题给出和 Burnside 对上述问题相同的回答，这是 C. Hobby 在 1960 年证明的 (近二十多年来，对于这两个问题又有了很多研究). 另外 Blackburn 在 1957 年还证明了下述结果：设 G 是有限 p- 群，若 $d(G')=2$, G' 非交换，则 G' 为类 2 亚循环群. 又若 $d(G)=d(G')=2$, 则 G' 交换. 可参看下文：

N. Blackburn, On prime-power groups in which the derived group has two generators, *Proc. Cambr. Phil. Soc.* **53**(1957), 19–27.

最后，我们来决定具有循环极大子群的有限 p- 群.

定理 5.14 设 $|G|=p^n$, G 有 p^{n-1} 阶循环子群 $\langle a\rangle$, 则 G 只有下述七种类型：

(I) p^n 阶循环群： $G=\langle a\rangle$, $a^{p^n}=1$, $n\geq 1$.

(II) (p^{n-1},p) 型交换群： $G=\langle a,b\rangle$ $a^{p^{n-1}}=b^p=1$, $[a,b]=1$, $n\geq 2$.

(III) $p\neq 2$, $n\geq 3$, $G=\langle a,b\rangle$, 有定义关系：

$$a^{p^{n-1}}=1,\ b^p=1,\ b^{-1}ab=a^{1+p^{n-2}}.$$

(IV) 广义四元数群： $p=2$, $n\geq 3$, $G=\langle a,b\rangle$, 有定义关系：

$$a^{2^{n-1}}=1,\ b^2=a^{2^{n-2}},\ b^{-1}ab=a^{-1}.$$

(V) 二面体群： $p=2$, $n\geq 3$, $G=\langle a,b\rangle$, 有定义关系：

$$a^{2^{n-1}}=1,\ b^2=1,\ b^{-1}ab=a^{-1}.$$

(VI) $p=2$, $n\geq 4$, $G=\langle a,b\rangle$, 有定义关系：

$$a^{2^{n-1}}=1,\ b^2=1,\ b^{-1}ab=a^{1+2^{n-2}}.$$

(VII) $p=2$, $n\geq 4$, $G=\langle a,b\rangle$, 有定义关系：

$$a^{2^{n-1}}=1,\ b^2=1,\ b^{-1}ab=a^{-1+2^{n-2}}.$$

证 除去交换的情形, 有 $n \geq 3$. 我们先假定 $p > 2$. 设 $\langle a \rangle$ 是 G 的循环极大子群, 当然有 $\langle a \rangle \trianglelefteq G$. 任取 $b_1 \notin \langle a \rangle$, 有 $b_1^p \in \langle a \rangle$. 设 $b_1^{-1}ab_1 = a^r$, 由 G 非交换, 有 $r \not\equiv 1 \pmod{p^{n-1}}$. 又由 $b_1^p \in \langle a \rangle$, 有 $b_1^{-p}ab_1^p = a^{r^p} = a$, 于是 $r^p \equiv 1 \pmod{p^{n-1}}$. 即 r 在模 p^{n-1} 的简化剩余系的乘法群中是 p 阶元素, 由此易推出, $r \equiv 1 \pmod{p^{n-2}}$. 于是可令 $r = 1 + kp^{n-2}$. 因 $r \not\equiv 1 \pmod{p^{n-1}}$, 有 $k \not\equiv 0 \pmod{p}$, 取整数 j 使 $jk \equiv 1 \pmod{p}$. 再令 $b_2 = b_1^j$, 有

$$b_2^{-1}ab_2 = b_1^{-j}ab_1^j = a^{r^j} = a^{(1+kp^{n-2})^j} = a^{1+p^{n-2}}.$$

又因 $b_2^p \in \langle a \rangle$, 而 $o(b) \leq p^{n-1}$, 可令 $b_2^p = a^{sp}$, s 是整数, 我们要证明 $(b_2a^{-s})^p = 1$. 这因为 $\langle a^{p^{n-2}} \rangle$ char $\langle a \rangle$, 得到 $\langle a^{p^{n-2}} \rangle \trianglelefteq G$, 于是 $\langle a^{p^{n-2}} \rangle \leq Z(G)$. 又 $[a,b] = a^{p^{n-2}}$, 所以 $[a,b]^g = a^{p^{n-2}}$, 对任意的 $g \in G$. 由定理 1.8(3) 有 $G' = \langle a^{p^{n-2}} \rangle$, 于是 $G' \leq Z(G)$, $c(G) = 2$. 据第 I 章 §4 习题 10, 有

$$(xy)^p = x^p y^p [y,x]^{\binom{p}{2}} = x^p y^p, \ \forall x, y \in G.$$

于是由 $b_2^p = a^{sp}$ 可得 $(b_2a^{-s})^p = b_2^p a^{-sp} = 1$. 令 $b = b_2a^{-s}$, 即可得 G 有定义关系 (III).

下面设 $p = 2$. 同样设 $\langle a \rangle$ 是 G 的循环极大子群, 而 $b \notin \langle a \rangle$. 则 $b^2 \in \langle a \rangle$, 且 $b^{-1}ab = a^r$, 其中 $r \not\equiv 1 \pmod{2^{n-1}}$, 但 $r^2 \equiv 1 \pmod{2^{n-1}}$. 由此推出 r 模 2^{n-1} 只有三种可能: $r = -1$, $r = 1+2^{n-2}$ 和 $-1+2^{n-2}$. 又由 $b^2 \in \langle a \rangle$, 可令 $b^2 = a^s$. 因 $b^{-1}(b^2)b = b^2$, 即 $b^{-1}a^sb = a^s$, 有 $a^{sr} = a^s$, 即 $sr \equiv s \pmod{2^{n-1}}$. 若 $r = -1$, 则 $s \equiv -s \pmod{2^{n-1}}$, 推出 $a^s = 1$ 或 $a^{2^{n-2}}$, 这分别给出广义四元数群 (IV) 和二面体群 (V). 当 $n = 3$ 时, 第 II 章 §3 中已经决定了 2^3 阶非交换群, 只有上述两种类型. 而对于 $n \geq 4$, 还要讨论 $r = \pm 1 + 2^{n-2}$ 的情况. 若 $r = 1 + 2^{n-2}$, 条件 $sr \equiv s \pmod{2^{n-1}}$ 等价于 s 是偶数. 令 $s = 2t$, 由同余式 $j(1+2^{n-3}) + t \equiv 0 \pmod{2^{n-2}}$ 能决定 j. 设 $b_1 = ba^j$, 则

$$b_1^2 = b^2(b^{-1}a^jb)a^j = b^2a^{j(2+2^{n-2})} = a^{2[j(1+2^{n-3})+t]} = 1,$$

而 $b_1^{-1}ab_1 = a^{1+2^{n-2}}$, 对 b_1 和 a 来说就满足定义关系 (VI). 若 $r = -1 + 2^{n-2}$, 条件 $sr \equiv s \pmod{2^{n-1}}$ 变成 $(-2 + 2^{n-2})s \equiv 0 \pmod{2^{n-1}}$, 即 $(-1 + 2^{n-3})s \equiv 0 \pmod{2^{n-2}}$, 于是得到 $s \equiv 0 \pmod{2^{n-2}}$, 这样 $b^2 = 1$ 或 $a^{2^{n-2}}$. 而若 $b^2 = a^{2^{n-2}}$, 令 $b_1 = ba$, 则

$$b_1^2 = (ba)^2 = b^2(b^{-1}ab)a = b^2a^{-1+2^{n-2}}a = a^{2^{n-2}}a^{2^{n-2}} = 1,$$

因此 a 和 b 或者 a 和 b_1 满足定义关系 (VII).

最后要说明上述七种类型的群彼此互不同构. 因为第 II 章 §3 中已经讨论过阶 $\leq p^3$ 的 p- 群, 故这里可设 $n \geq 4$. 区别交换和不交换以及 $p > 2$ 和 $p = 2$ 的情形, 只须说明 (IV)–(VII) 之间互不同构即可. 由定义关系可看出, 对这四种情况都有 $G' = \langle [a, b] \rangle$. 计算 $[a, b]$ 得

$$[a,b] = a^{-1}b^{-1}ab = \begin{cases} a^{-2}, & \text{对于 (IV), (V)}, \\ a^{2^{n-2}}, & \text{对于 (VI)}, \\ a^{-2+2^{n-2}}, & \text{对于 (VII)}. \end{cases}$$

于是对于 (VI), 有 $|G'| = 2$, 而对其余情形, 有 $|G'| = 2^{n-2}$, 故 (VI) 不与其余三种情形同构. 再计算 $\langle a \rangle$ 外一般元素 ba^i 的平方, 得

$$(ba^i)^2 = b^2(b^{-1}a^ib)a^i = \begin{cases} 1, & \text{对于 (IV)}, \\ a^{2^{n-2}}, & \text{对于 (V)}, \\ a^{i2^{n-2}}, & \text{对于 (VII)}. \end{cases}$$

这首先说明 G 中 2^{n-1} 阶循环子群是唯一的. 其次, $\langle a \rangle$ 外的元素对于 (IV) 来说全是 2 阶的; 对于 (V), 全是 4 阶的; 而对于 (VII), 既有 2 阶元也有 4 阶元. 由此看出 (IV), (V), (VII) 之间互不同构. □

§6. p- 群计数定理

所谓 p- 群的计数定理是指关于有限 p- 群各种类型的子群、元素或子集个数的结果. 反过来, 由 p- 群子群个数的条件推出 p-

群本身的性质或结构也是 p- 群计数问题的课题. 本节介绍几个重要的经典结果, 它们都是在本世纪三十年代以前得到的.

设 G 是有限 p- 群, $|G| = p^n$. 对于 $k = 0, 1, \cdots, n$, 以 $s_k(G)$ 表示 G 中 p^k 阶子群的个数, 而以 $c_k(G)$ 表 G 中 p^k 阶循环子群的个数.

定理 6.1 *设 $|G| = p^n$, 若 $s_1(G) = 1$, 则*
(1) 对 $p > 2$, G 是循环群;
(2) 对 $p = 2$, G 是循环群或广义四元数群.

证 根据引理 5.9, 若 G 非循环, 对 $p > 2$, G 中存在 (p, p) 型正规子群, 于是 $s_1(G) > 1$, 与假设矛盾, 定理得证. 而对 $p = 2$, 由定理 5.10(2) 以及 $s_1(G) = 1$ 可推出 G 中存在循环极大子群. 再由定理 5.14, G 若不循环, 必为 (IV)-(VII) 型群. 计算 $(ba^i)^2$, 并考察 $(ba^i)^2 = 1$ 的解, 可知除 (V) 型群外, 其余三种在 $\langle a \rangle$ 外都有二阶元素, 于是 $s_1(G) > 1$. 因此 G 只能为循环群或广义四元数群. □

定理 6.2 *设 $|G| = p^n$, $1 < m < n$. 若 $s_m(G) = 1$, 则 G 循环.*

证 设 H 是 G 的唯一的 p^m 阶子群. 任取 G 的 p^{m+1} 阶子群 $H_1 > H$, 由 H 是 H_1 的唯一的极大子群, 知 $H = \Phi(H_1)$, 又由 $|H_1/\Phi(H_1)| = p$ 知 H_1 循环, 于是 H 也是循环群. 这又推出只要 $i \le m$, 都有 $s_i(G) = 1$. 特别地, 有 $s_1(G) = 1$. 据定理 6.1, 得 G 循环或为广义四元数群. 但对后者有 $s_2(G) > 1$, 与 $s_2(G) = 1$ 矛盾, 于是 G 不能为广义四元数群, 即 G 必为循环群. □

定理 6.3 *设 $|G| = p^n$, $1 < m \le n$. 若 $s_m(G) = c_m(G)$, 即 G 的每个 p^m 阶子群皆为循环群, 则 G 循环, 或当 $p^m = 4$ 时 G 可能为广义四元数群.*

证 因 $m \ge 2$, 所有 p^2 阶子群循环 (因每个 p^2 阶子群至少含于一个 p^m 阶子群), 于是必有 $s_1(G) = 1$.(若否, 我们可找到两个不同的 p 阶子群 C_1, C_2, 并可设其中之一含于 $Z(G)$, 于是

$\langle C_1, C_2\rangle = C_1 \times C_2$ 是 (p,p) 型群，矛盾.) 应用定理 6.1, G 为循环群或广义四元数群. 但对后者，如果 $m \geq 3$, G 中存在非循环的 p^m 阶子群 $\langle a^{2^{n-m}}, b\rangle$, 与假设矛盾. □

为了进一步研究 p- 群的计数定理，我们把 I, 例 7.7 叙述成下面的

引理 6.4 设 G 是 p^n 阶初等交换 p- 群，$0 \leq m < n$, 则 G 中 p^m 阶子群为

$$\begin{bmatrix} n \\ m \end{bmatrix}_p = \begin{cases} \frac{(p^n-1)(p^{n-1}-1)\cdots(p^{n-m+1}-1)}{(p^m-1)(p^{m-1}-1)\cdots(p-1)}, & m > 0, \\ 1, & m = 0. \end{cases}$$

为了方便，我们规定若 $n < m$, 则 $\left[\begin{smallmatrix} n \\ m \end{smallmatrix}\right]_p = 0$. 于是对任意的非负整数 n, m, 都规定了一个非负整数 $\left[\begin{smallmatrix} n \\ m \end{smallmatrix}\right]_p$. 又若在我们的问题只涉及一个素数 p, 我们常把 $\left[\begin{smallmatrix} n \\ m \end{smallmatrix}\right]_p$ 的下标 p 省略，而简记 $\left[\begin{smallmatrix} n \\ m \end{smallmatrix}\right]$. 下面是关于数 $\left[\begin{smallmatrix} n \\ m \end{smallmatrix}\right]_p$ 的一些主要性质.

引理 6.5 (1) 若 $n \geq m$, 则 $\left[\begin{smallmatrix} n \\ m \end{smallmatrix}\right] = \left[\begin{smallmatrix} n \\ n-m \end{smallmatrix}\right]$;

(2) 对任意的 n, m, $\left[\begin{smallmatrix} n+1 \\ m \end{smallmatrix}\right] = \left[\begin{smallmatrix} n \\ m \end{smallmatrix}\right] + p^{n-m+1}\left[\begin{smallmatrix} n \\ m-1 \end{smallmatrix}\right]$;

(3) 若 $n \geq m$, 则 $\left[\begin{smallmatrix} n \\ m \end{smallmatrix}\right] \equiv 1 \pmod p$;

(4) 若 $n > m > 0$, 则 $\left[\begin{smallmatrix} n \\ m \end{smallmatrix}\right] \equiv 1 + p \pmod{p^2}$;

(5) $(x-1)(x-p)\cdots(x-p^{n-1})$

$$= \sum_{i=0}^{n} (-1)^i p^{\binom{i}{2}} \begin{bmatrix} n \\ i \end{bmatrix} x^{n-i};$$

(6) $\sum_{i=0}^{n} (-1)^i p^{\binom{i}{2}} \left[\begin{smallmatrix} n \\ i \end{smallmatrix}\right] = 0$.

证 (1), (2) 可直接用公式验证.

(3), (4): 利用 (2) 式可得

$$\begin{bmatrix} n \\ m \end{bmatrix} \equiv \begin{bmatrix} n-1 \\ m \end{bmatrix} \equiv \cdots \equiv \begin{bmatrix} m \\ m \end{bmatrix} = 1 \pmod p$$

和

$$\begin{aligned}\begin{bmatrix}n\\m\end{bmatrix} &\equiv \begin{bmatrix}n-1\\m\end{bmatrix}\equiv\cdots\equiv\begin{bmatrix}m+1\\m\end{bmatrix}\\ &= \begin{bmatrix}m+1\\1\end{bmatrix}\equiv 1+p\ (\mathrm{mod}\ p^2).\end{aligned}$$

(5) 用对 n 的归纳法，细节略.

(6) 在 (5) 中令 $x=1$ 即得所需结果. □

设 G 是有限 p- 群， $\Phi(G)$ 为 G 的 Frattini 子群. 称 G 的包含 $\Phi(G)$ 的子群为 G 的 大子群(major subgroup). 对于 $i=0,1,\cdots,d=d(G)$, 令 $\mathcal{S}_i$ 表示 G 的指数为 p^i 的大子群的集合. 又令 $\mathfrak{S}$ 是一个由 G 的真子群组成的任意集合，以 $s(M)$ 表示 $\mathfrak{S}$ 中含于 M 的子群个数. 则有下述重要结果:

定理 6.6 (P. Hall 计数原则)

$$\begin{aligned}&s(G)-\sum_{M\in\mathcal{S}_1}s(M)+p\sum_{M\in\mathcal{S}_2}s(M)-\cdots\\ &\quad+(-1)^d p^{\binom{d}{2}}s(\Phi(G))=0.\end{aligned}\tag{6.1}$$

证 设 H 是 $\mathfrak{S}$ 中任一子群. 考虑 G 的所有包含 H 的大子群的交 N, 当然 N 也是 G 的大子群. 设 $N\in\mathcal{S}_i$, 则必有 $i\geq 1$ (因 G 的真子群 H 至少属于 G 的一个极大子群). 于是，每个包含 N 的大子群都包含 H. 对于 $1\leq j\leq i$, $\mathcal{S}_j$ 中包含 N 的大子群个数应为 $\begin{bmatrix}i\\j\end{bmatrix}$, 于是 H 在 (6.1) 式左端出现的重数为

$$\begin{aligned}m(H) &= 1-\begin{bmatrix}i\\1\end{bmatrix}+p\begin{bmatrix}i\\2\end{bmatrix}-\cdots\\ &\quad+(-1)^i p^{\binom{i}{2}}\begin{bmatrix}i\\i\end{bmatrix}.\end{aligned}$$

由引理 6.5(6), $m(H)=0$. 当 H 取遍 $\mathfrak{S}$ 中所有子群，并求和便得 (6.1) 式右端 $=\sum_{H\in\mathfrak{S}}m(H)=0$, 证毕. □

下面证明两个著名的计数定理.

定理 6.7 设 $|G| = p^n$, $0 \le k \le n$, 则 $s_k(G) \equiv 1 \pmod p$.

证 当 $k = 0$ 和 n 时, 定理显然成立. 现在设 $0 < k < n$, 用对 n 的归纳法. 设 M 是 G 的任一极大子群, 由归纳假设, $s_k(M) \equiv 1 \pmod p$. 令 $\mathfrak{S}$ 为 G 的所有 p^k 阶子群的集合, 应用 P. Hall 计数原则, 得到

$$s_k(G) \equiv \sum_{M \in \mathcal{S}_1} s_k(M) \equiv \sum_{M \in \mathcal{S}_1} 1 = \begin{bmatrix} d \\ d-1 \end{bmatrix} \equiv 1 \pmod p.$$

□

定理 6.8 (Kulakoff) 设 $p > 2$, $|G| = p^n$, 且 G 非循环. 若 $1 \le k \le n-1$, 则 $s_k(G) \equiv 1 + p \pmod{p^2}$.

为证明此定理, 先证明

引理 6.9 设 $|G| = p^n, p > 2, n \ge 3$. 若 G 有循环极大子群, 但 G 非循环, 则 G 恰有 p 个循环极大子群和一个非循环极大子群.

证 由引理条件, G 应为定理 5.14 中 (II) 或 (III) 型群. 由定义关系易看出 $d(G) = 2, c(G) \le 2$. 据第 I 章 §4 习题 10, G 中成立 $(xy)^p = x^p y^p$, 对任意的 $x, y \in G$. 这样, 对 $i = 0, 1, \cdots, p-1$, 有

$$(b^i a)^p = b^{ip} a^p = a^p,$$

即 $b^i a$ 是 p^{n-1} 阶元素, 这就找到了 p 个循环极大子群 $\langle b^i a \rangle$. 又, 易验证 $\langle a^p, b \rangle$ 是 G 的 (p^{n-2}, p) 型交换极大子群, 自然非循环. 再据 $d(G) = 2$, G 中恰有 $1 + p$ 个极大子群, 引理得证. □

定理 6.8 的证明 当 $n = 2$, G 是 (p, p) 型交换群. 有 $1 + p$ 个 p 阶子群, 定理显然成立. 下面设 $n > 2$. 用对 n 的归纳法. 首先, 当 $k = n - 1$ 时, 因 $d = d(G) \ge 2$, 有

$$s_{n-1}(G) = \begin{bmatrix} d \\ d-1 \end{bmatrix} = \begin{bmatrix} d \\ 1 \end{bmatrix} \equiv 1 + p \pmod{p^2}.$$

而当 $k \le n-2$ 时，用 P. Hall 计数原则，有

$$s_k(G) \equiv \sum_{M \in \mathcal{S}_1} s_k(M) - p \sum_{M \in \mathcal{S}_2} s_k(M) \pmod{p^2}.$$

对 $M \in \mathcal{S}_2$, 由定理 6.7, $s_k(M) \equiv 1 \pmod p$, 有

$$p \sum_{M \in \mathcal{S}_2} s_k(M) \equiv p \sum_{M \in \mathcal{S}_2} 1 = p \begin{bmatrix} d \\ d-2 \end{bmatrix} \equiv p \pmod{p^2}.$$

而对 $M \in \mathcal{S}_1$, 若每个 M 都非循环，应用归纳假设，有 $s_k(M) \equiv 1 + p \pmod{p^2}$. 于是

$$\begin{aligned} s_k(G) &\equiv (1+p)\begin{bmatrix} d \\ d-1 \end{bmatrix} - p \equiv (1+p)^2 - p \\ &\equiv 1 + p \pmod{p^2}. \end{aligned}$$

又，若有循环子群 $M \in \mathcal{S}_1$, 则由上述引理，$\mathcal{S}_1$ 中恰含 p 个循环子群和一个非循环子群，于是

$$s_k(G) \equiv p \cdot 1 + (1+p) - p \equiv 1 + p \pmod{p^2}.$$

习　题

1. 设 A, B, C 是群 G 的子群，若 $B \le N_G(A) \cap N_G(C)$, 则 $[AB, C] = [A, C][B, C]$.

2. 设 $A \trianglelefteq G$, $B \le G$, $C \le G$. 则 $[AB, AC] \le A[B, C]$.

3. 设 A 是群 G 的交换正规子群，且其商群 $G/A = \langle xA \rangle$ 是循环群. 则

(1) 映射 $a \mapsto [a, x]$, $a \in A$, 是 A 到 G' 上的满同态;

(2) $G' \cong A/A \cap Z(G)$.

4. 设 G 是有限群，满足 $G'' = 1$, 且 G/G' 循环. 则对每个满足 $G = \langle G', x \rangle$ 的元素 x 都有 $o(x) = |G/G'|$, 因此 $\langle x \rangle$ 是 G' 在 G 中的补群.

5. 称群 G 为 **亚交换群**, 如果 $G'' = 1$, 或者等价地，G' 是交换群. 证明亚交换群 G 中有下列换位子公式：设 $a, b, c \in G$.

(1) 若 $b \in G'$, 则

$$[ab, c] = [a, c][b, c],$$
$$[c, ab] = [c, a][c, b];$$

(2) 若 $c \in G'$, n 为正整数，则

$$[c^{-1}, a] = [c, a]^{-1}, \quad [c^n, a] = [c, a]^n;$$

(3) $[a, b^{-1}, c]^b = [b, a, c]$;

(4) $[a, b, c][b, c, a][c, a, b] = 1$;

(5) 若 $c \in G'$, 则

$$[c, a, b] = [c, b, a].$$

6. 设 $G = \langle a, b \rangle$ 是亚交换群: $n \geq 2$. 则 G_n/G_{n+1} 可由 $n-1$ 个元素生成.

7. 设 G 是二元生成群，则 $G'' \leq G_5$.

8. 举例说明由 N 及 G/N 的幂零性不能得出 G 的幂零性.

9. 设 G/M 和 G/N 幂零，则 $G/M \cap N$ 亦幂零.

10. 有限群 G 幂零的充要条件为 G 的任一子群为次正规子群.

11. 有限群 G 幂零的充要条件为: 对任意的 $x, y \in G$, 只要 $(o(x), o(y)) = 1$ 就有 $[x, y] = 1$.

12. 有限群 G 幂零的充要条件为 G 的任一二元生成子群幂零.

13. 设 G 是有限群，命 $O^p(G)$ 为 G 之所有 Sylow q- 子群生成的子群，其中 $q \bigm| |G|$, 且 $q \neq p$. 则

(1) $O^p(G) \trianglelefteq G$, $G = O^p(G)P$, 其中 $P \in \mathrm{Syl}_p(G)$;

(2) $G/O^p(G)$ 是 p- 群;

(3) 若 $N \trianglelefteq G$, G/N 是 p- 群，则 $O^p(G) \leq N$;

(4) $O^p(G) = \bigcap\{N \bigm| N \trianglelefteq G \text{ 且} G/N \text{ 为 } p\text{- 群}\}$.

14. 设 G 是群，令

$$G_\infty = \bigcap_{i=1}^{\infty} G_i,$$

并称之为 G 的幂零余. 证明 G_∞ char G, 且

$$G_\infty = \bigcap\{N \bigm| N \trianglelefteq G \text{ 且} G/N \text{ 为幂零群}\}.$$

15. 设 G 是有限群，G_∞ 为 G 之幂零余. 则存在正整数 n 使得 $G_\infty = G_n$. 证明:

(1) G/G_∞ 幂零;

(2) 若 $N \trianglelefteq G$, G/N 幂零，则 $G_\infty \leq N$;

(3) $G_\infty = \bigcap_{p||G|} O^p(G)$;

(4) $G_\infty = \langle N \trianglelefteq G \bigm| [N, G] = N \rangle$.

16. 设 G 是群，令

$$Z_\infty(G)=\bigcup_{i=0}^{\infty}Z_i(G),$$

并称之为 G 的超中心. 证明 $Z_\infty(G)\ \mathrm{char}\ G$, 且若 G 为有限群，则存在正整数 n 使 $Z_\infty(G)=Z_n(G)$, 并且 G 幂零的充要条件为 $Z_\infty(G)=G$.

17. 设 G 是有限群， $Z_\infty(G)$ 为 G 之超中心. 则

$$Z_\infty(G)=\bigcap\{N \mid N\trianglelefteq G \text{ 且 } Z(G/N)=1\}.$$

18. 第 15 题的结论 (1) 和第 16 题最后的结论对无限群来说是否仍然成立？试举例说明之.

19. 设 G 是有限群， $Z_\infty(G)$ 为 G 的超中心. 又设 A 是 G 的幂零子群，则 $Z_\infty(G)A$ 亦幂零.

20. 设 G 是有限群， P 是 G 的一个正规 p- 子群使得 $G/C_G(P)$ 是 p-群，则 $P\le Z_\infty(G)$.

21. 设 G 是群, 满足 $G_\infty=1$. 则对任意的 $x,y\in G$, 只要 $(o(x),o(y))=1$ 就有 $[x,y]=1$.

22. 设 G 是群， i 是正整数. 若 $\exp(Z_i(G)/Z_{i-1}(G))$ 存在，则

$$\exp(Z_{i+1}(G)/Z_i(G))\ \Big|\ \exp(Z_i(G)/Z_{i-1}(G)).$$

类似地，若 $\exp(G_{i-1}/G_i)$ 存在，则

$$\exp(G_i/G_{i+1})\ \Big|\ \exp(G_{i-1}/G_i).$$

23. 证明由 $G=G'$ 可推出 $Z_2(G)=Z_1(G)$. 并对任意给定正整数 n, 构造群 G 满足 $Z(G)=1$, 但

$$G=G_1>G_2>G_3>\cdots>G_n.$$

24. 设 G 是无限群. 仍规定 $\Phi(G)$ 为 G 的所有极大子群的交；而如果 G 不存在极大子群，则规定 $\Phi(G)=G$. 证明定理 3.3 对无限群仍然成立.

25. 设 $N\trianglelefteq G$, 则 $\Phi(G)N/N\le\Phi(G/N)$. 若又有 $N\le\Phi(G)$, 则 $\Phi(G)/N=\Phi(G/N)$. 举例说明若 $N\not\le\Phi(G)$, 不一定有 $\Phi(G)N/N=\Phi(G/N)$.

26. 证明 $\Phi(G_1\times G_2)=\Phi(G_1)\times\Phi(G_2)$.

27. 设 G 是有限群，其中每个素数阶元素以及每个 4 阶元素属于 G 之中心，则 G 必为幂零群. 但如果仅假定 G 的每个素数阶元素属于中心，则不能推得 G 的幂零性. 试举例说明之.

28. 设 G 为有限极小非幂零群 (在第 III 章 §6 的意义下), 则 $|G| = p^n q$, $p \neq q$ 为素数, 且 G 的 Sylow p- 子群 P 为初等交换 p- 群, 并且是 G 的唯一的极小正规子群.

29. 设 G 是有限内交换群, 但 G 不是 p- 群. 则 G 必为内幂零群, 且其中的正规 Sylow 子群为初等交换群.

30. 设 G 是有限内交换 p- 群. 则

(1) G 是二元生成的;

(2) $\Phi(G) = Z(G)$, 且 $G/Z(G)$ 是 (p, p) 型初等交换群;

(3) $c(G) = 2$.

31. 设 G 是有限非交换群, 则 G 中必有一对共轭元素 x 和 x^g 使得 $x \neq x^g$, 但 $[x, x^g] = 1$.

32. 设 G 是有限 2- 群, 则 $\Phi(G) = \mho_1(G)$.

33. 设 G 是有限 p- 群, $|G| = p^n$. 又设 A 是 G 的一个极大的交换正规子群, 且 $|A| = p^a$. 则

(1) $C_G(A) = A$;

(2) $2n \leq a(a+1)$;

(3) $G_a \leq A$, $G_{2a} = 1$;

(4) 再设 A_1, A_2 是 G 的两个极大的交换正规子群, 且 $\exp A_i = p^{e_i}$, $i = 1, 2$. 则 $e_2 \leq 2e_1$.

34. 举例说明上题 (2) 中的等号可能成立.

35. 设有限 p- 群 G 有两个极大子群是交换的, 则 G 至少有 $p+1$ 个极大子群是交换的, 并且有 $c(G) \leq 2$.

36. 设 G 是有限 p- 群, $p > 2$. 若 $Z_2(G)$ 循环, 则 G 本身必循环.

37. 设有限 p- 群 G 有指数为 p^2 的交换子群, 则必有同指数的交换正规子群.

第 V 章

可解群

§1. π- 可分群，π- 可解群和可解群

设 π 是一个素数集合，π' 是 π 在全体素数集合中的补集. 若 π 只由一个素数 p 组成，我们把 $\{p\}$ 和 $\{p\}'$ 简记作 p 和 p'.

定义 1.1 称有限群 G 为 π- 群，如果 $|G|$ 的每个素因子均在 π 中，亦即 $|G|_\pi = |G|$. 对于 $\pi = \{p\}$, π- 群即以前定义的 p- 群. 又称元素 $x \in G$ 为 π- 元素，如果 $\langle x \rangle$ 是 G 的 π- 子群. 同样地，对于 $\pi = \{p\}$, π- 元素即以前定义的 p- 元素.

引理 1.2 设 M, N 是 G 的正规 π- 子群，则 $\langle M, N \rangle = MN$ 亦然.

证 显然 $MN \trianglelefteq G$. 又因为 $|MN| = \frac{|M||N|}{|M \cap N|}$, 由 M, N 是 π- 子群得知 $M \cap N$ 是 π- 子群，因而 $|MN|$ 的素因子全在 π 中，故 MN 是 π- 子群. □

由此引理，G 的所有正规 π- 子群生成的子群仍为 G 的正规 π- 子群，记作 $O_\pi(G)$. 它是 G 中最大的正规 π- 子群，也是 G 的特征子群.

引理 1.3 $O_\pi(G/O_\pi(G)) = 1$.

证 $G/O_\pi(G)$ 的正规 π- 子群在自然同态 $G \to G/O_\pi(G)$ 下的原像仍为 G 的正规 π- 子群，故得结论. □

定义 1.4 称有限群 G 为 π- 可分群，如果存在 G 的一个正规群列

$$G = N_0 \geq N_1 \geq N_2 \geq \cdots \geq N_r = 1, \tag{1.1}$$

使 N_i/N_{i+1} 为 π- 群或 π'- 群，$i = 0, 1, \cdots, r-1$.

而称 G 为 π- 可解群，如果 G 中存在正规群列 (1.1)，使 N_i/N_{i+1} 为 π'- 群或 p- 群，其中 $p \in \pi$, $i = 0, 1, \cdots, r-1$.

明显地，G 是 π- 可分群等价于 G 是 π'- 可分群，但对 π- 可解群，则没有这样的对称性.

另一方面，根据 Feit-Thompson 定理，若 $2 \notin \pi$，则 π- 可分群即 π- 可解群. 又，对任意的素数 p, p- 可分群和 p- 可解群这两个概念也是一致的.

定理 1.5 设 G 是 π- 可分群 (π- 可解群). 则

(1) G 的每个子群是 π- 可分群 (π- 可解群);

(2) G 的每个商群是 π- 可分群 (π- 可解群);

(3) G 的极小正规子群是 π'- 群或 π- 群 (π'- 群或 p- 群；其中 $p \in \pi$);

(4) 对任意的 $N \lhd G$, $N \neq G$, 有 $O_\pi(G/N) \neq 1$ 或 $O_{\pi'}(G/N) \neq 1$ ($O_{\pi'}(G/N) \neq 1$ 或 $O_p(G/N) \neq 1$, 对某个 $p \in \pi$.)

证 我们只对 π- 可分群来证明上述结论.

因为 G π- 可分，G 有正规群列

$$G = N_0 \geq N_1 \geq N_2 \geq \cdots \geq N_r = 1,$$

其中每个 N_i/N_{i+1} 是 π- 群或 π'- 群.

(1) 若 $H \leq G$, 则

$$H = H \cap N_0 \geq H \cap N_1 \geq \cdots \geq H \cap N_r = 1$$

是 H 的正规群列. 并且

$$\begin{aligned} H \cap N_i / H \cap N_{i+1} &= H \cap N_i / (H \cap N_i) \cap N_{i+1} \\ &\cong (H \cap N_i) N_{i+1} / N_{i+1} \end{aligned}$$

是 N_i/N_{i+1} 的子群，故其为 π- 群或 π'- 群.

(2) 若 $H \lhd G$, $H \neq G$, 则

$$G/H = N_0H/H \geq N_1H/H \geq \cdots \geq N_rH/H = 1$$

是 G/H 的正规群列. 并且

$$\begin{aligned} N_iH/H \ / \ N_{i+1}H/H &\cong N_iH/N_{i+1}H \\ &\cong N_i/N_i \cap N_{i+1}H \end{aligned}$$

是 N_i/N_{i+1} 的商群，故其为 π- 群或 π'- 群.

(3) 由 π- 可分性的定义， G 的所有主因子都是 π- 群或 π'- 群. 于是 G 的每个极小正规子群亦为 π- 群或 π'- 群.

(4) 因为 G/N 是 π- 可分群，取 G/N 的一个极小正规子群 M/N, 则必为 π- 群或 π'- 群. 因此，或者 $O_\pi(G/N) \neq 1$, 或者 $O_{\pi'}(G/N) \neq 1$. □

对于任意群，我们以 $O_{\pi\pi'}(G)$ 表 $O_{\pi'}(G/O_\pi(G))$ 在 G 中的原像. 同样地，以 $O_{\pi\pi'\pi}(G)$ 表 $O_\pi(G/O_{\pi\pi'}(G))$ 在 G 中的原像，依此类推. 由引理 1.3 及定理 1.5(4), 如果 G 是 π- 可分群，则群列

$$1 \leq O_\pi(G) \leq O_{\pi\pi'}(G) \leq O_{\pi\pi'\pi}(G) \leq \cdots$$

必终止于 G. 这样，对 π- 可分群还可得到一个因子群为 π- 群或 π'- 群的特征群列. 同样可以证明，对于 π- 可解群可得到一其因子群为 π'- 群或 p- 群， $p \in \pi$ 的特征群列.

定理 1.6 *由下列条件之一即可推出 G 是 π- 可分群 (π- 可解群).*

(1) 存在 G 的 π- 可分 (π- 可解) 正规子群 N, 使 G/N 为 π- 可分 (π- 可解) 群;

(2) 对任意的 $N \lhd G$, $N \neq G$, G/N 的极小正规子群均为 π- 群 (p- 群， $p \in \pi$) 或 π'- 群;

(3) 对任意的 $N \lhd G$, $N \neq G$, 或者 $O_\pi(G/N) \neq 1$ ($O_p(G/N) \neq 1, p \in \pi$), 或者 $O_{\pi'}(G) \neq 1$.

证 我们也只对 π- 可分群来证明这个定理.

(1) 由 G/N π- 可分，存在 G 到 N 的正规群列，使其因子群为 π- 群或 π'- 群. 又由 N π- 可分，可得 N 的一个特征群列，其因子群为 π- 群或 π'- 群. 把这两个群列接起来，就得到 G 的一个正规群列，其因子群为 π- 群或 π'- 群，于是 G π- 可分.

(2) 对 $|G|$ 用归纳法. 设 K 是 G 的极小正规子群，则 K 是 π- 群或 π'- 群. 并且定理条件对 G/K 亦满足. 因为 $|G/K| < |G|$, 由归纳假设得 G/K 是 π- 可分群. 由 (1) 又得 G 的 π- 可分性.

(3) 对 $|G|$ 用归纳法. 由条件先有 $O_\pi(G) \neq 1$ 或 $O_{\pi'}(G) \neq 1$. 不妨设 $O_\pi(G) \neq 1$. 则 $G/O_\pi(G)$ 亦满足定理条件, 并且 $|G/O_\pi(G)| < |G|$. 由归纳假设，$G/O_\pi(G)$ π- 可分，由 (1) 又得 G 的 π- 可分性. □

请读者对于 π- 可解的情形证明上面的定理 1.5 和定理 1.6.

下面继续研究可解群. 在第 I 章 §4 中定义了可解群，并证明了它们的一些简单性质. 后来，在第 III 章 §1 中又证明了 G 可解的充要条件为 G 的合成因子皆为素数阶循环群，从而 G 的主因子对某个素数 p 必为初等交换 p- 群. 下面我们再证明

定理 1.7 *设 G 是有限群，则下述事项等价：*

(1) G 可解;

(2) 对每个素数集合 π, G 都是 π- 可分群 (或 π- 可解群);

(3) 对每个素数 p, G 都是 p- 可解群;

(4) 对任意的 $1 \neq N \lhd G$, 存在素数 p 使 $O_p(G/N) \neq 1$;

(5) 对任意的 $1 \neq N \lhd G$, 存在 G/N 的特征子群 $K/N \neq 1$, 使 K/N 是初等交换 p- 群.

证 (1) ⇒ (2): 任给 G 的主群列，因 G 可解，每个主因子皆为初等交换 p- 群. 故对任一素数集合 π, G 是 π- 可分的，也是 π- 可解的.

(2) ⇒ (3): 显然.

(3) ⇒ (4): 设 M/N 是 G/N 的使 $|M/N|$ 的素因子个数最少的极小正规子群，则 $|M/N|$ 素因子集合 $\pi = \{p\}$. 若否，便有素

数 $q \neq p$, $q \in \pi$, 则由 M/N 的 p- 可解性, 有 $O_p(M/N) \neq 1$ 或 $O_{p'}(M/N) \neq 1$. 这两个群都是 M/N 的特征子群, 因而是 G/N 的正规子群, 但它的阶的素因子个数 $< |\pi|$, 与 M/N 的取法矛盾.

(4) $\Rightarrow$ (5): 由 (4) 可假定对某素数 p, 有 $O_p(G/N) \neq 1$. 令 $U/N = \Omega_1(Z(O_p(G/N))) \neq 1$, 则 U/N 即满足要求.

(5) $\Rightarrow$ (1): 由 (5), G 存在正规群列, 使每个商群为初等交换 p- 群, 于是 G 可解. □

§2. π-Hall 子群

在第 III 章 §4 中我们对有限群定义了 π-Hall 子群 的概念. 对于 $\pi = \{p\}$, π-Hall 子群就是 p-Sylow 子群. 于是 Sylow 定理就是说, 对于任一素数 p, 有限群 G 的极大 p- 子群都是 p-Hall 子群, 并且任二 p-Hall 子群是共轭的. 但如果把 $\{p\}$ 换成任一素数集合 π, 则类似命题一般并不正确. 譬如设 $G = A_5$, $\pi = \{3, 5\}$, 则 G 中不存在 π-Hall 子群. (若存在 π-Hall 子群, 则它应为 15 阶. 但由 II,4.7 的证明知 G 中没有 15 阶子群.) 又设 $\pi = \{2, 3\}$, 则 G 中 6 阶子群 $\langle (123), (12)(45) \rangle$ 是极大 π- 子群, 但不是 π-Hall 子群 (这点留给读者作为习题). 最后设 $G = GL(3, 2) = PSL(3, 2)$ 是 168 阶单群 (参看附录研究题的 11), 把 G 看作 8 阶初等交换 2- 群 A 的自同构群, 则 G 传递地变换 A 的 7 个 2 阶子群, 也传递地变换 A 的 7 个 4 阶子群. 于是 G 关于某个 2 阶子群和某个 4 阶子群的稳定子群是 G 的两个不共轭的 $\{2, 3\}$-Hall 子群 (这点也留给读者作为习题).

但是, 对于 π- 可分群, 我们有

定理 2.1 设 G 是 π- 可分群, 则

(1) G 的 π-Hall 子群和 π'-Hall 子群总是存在的;

(2) 只要 G 的所有 π-Hall 子群或所有 π'-Hall 子群是可解的, 则 G 的所有 π-Hall 子群共轭, 并且 G 的所有 π'-Hall 子群也共轭;

(3) 在 (2) 的假定下，G 的任一 π- 子群都包含在某一 π-Hall 子群之中，并且对 π'- 子群也有类似结论.

证 (1) 由 G π- 可分，或者 $O_\pi(G) \neq 1$, 或者 $O_{\pi'}(G) \neq 1$. 因为 π- 可分性和 π'- 可分性等价，故不失普遍性可令 $O_\pi(G) \neq 1$. 考虑 $\overline{G} = G/O_\pi(G)$. 用归纳法，可假定 $\overline{G}$ 存在 π-Hall 子群 $H/O_\pi(G)$ 和 π'-Hall 子群 $U/O_\pi(G)$. 这时 H 即为 G 的 π-Hall 子群. 再应用 Schur-Zassenhaus 定理，U 中存在 π'-Hall 子群 K, 比较阶知 K 就是 G 的 π-Hall 子群.

(2) 和 (1) 相同可设 $O_\pi(G) \neq 1$, 考虑 $\overline{G} = G/O_\pi(G)$. 由于 $\overline{G}$ 的 π-Hall 子群和 π'-Hall 子群同构于 G 的相应子群的同态像，故定理的条件对 $\overline{G}$ 也成立. 于是用归纳法可假定 $\overline{G}$ 的所有 π-Hall 子群和 π'-Hall 子群彼此共轭. 这立即推出 G 的 π-Hall 子群彼此共轭. 而对 G 的任意的两个 π'-Hall 子群 K_1, K_2 有 $\overline{K_1} = K_1O_\pi(G)/O_\pi(G)$ 和 $\overline{K_2} = K_2O_\pi(G)/O_\pi(G)$ 是 $\overline{G}$ 的 π'-Hall 子群. 由 $\overline{K_1}$ 和 $\overline{K_2}$ 共轭，存在 $g \in G$ 使 $K_1^gO_\pi(G) = K_2O_\pi(G) = M$. 因为 K_1^g, K_2 是 M 的 π'-Hall 子群，据 Schur-Zassenhuas 定理得 K_1^g 和 K_2 在 M 中共轭，于是 K_1 和 K_2 在 G 中共轭.

(3) 由 π- 可分性和 π'- 可分性等价，只须对 π- 子群证明定理的结论. 用对 $|G|$ 的归纳法. 设 K 是 G 的任一 π- 子群. 由 G 的 π- 可分性，有 $O_\pi(G) \neq 1$ 或 $O_{\pi'}(G) \neq 1$. 分以下两种情形：

(i) 若 $O_\pi(G) \neq 1$, 考虑 $\overline{G} = G/O_\pi(G)$. 由归纳假设 $\overline{G}$ 的 π-子群 $KO_\pi(G)/O_\pi(G)$ 含于某个 π-Hall 子群 $H/O_\pi(G)$ 中，于是 $KO_\pi(G) \leq H, K \leq H$. 因为 H 也是 G 的 π-Hall 子群，定理得证.

(ii) 若 $O_{\pi'}(G) \neq 1$. 考虑 $\overline{G} = G/O_{\pi'}(G)$. 由归纳假设，$\overline{G}$ 的 π-子群 $KO_{\pi'}(G)/O_{\pi'}(G)$ 含于 $\overline{G}$ 的某个 π-Hall 子群 $M/O_{\pi'}(G)$ 中. 于是 $KO_{\pi'}(G) \leq M$. 若 $M < G$, 由归纳假设，K 含于 M 的某个 π-Hall 子群 H 中，比较阶知 H 亦为 G 之 π-Hall 子群，定理得证. 而若 $M = G$, 对于 G 之任一 π-Hall 子群 H, 令 $K_1 = KO_{\pi'}(G) \cap H$. 由 $G = O_{\pi'}(G) \cdot H = KO_{\pi'}(G) \cdot H$, 故

$$|G| = \frac{|K||O_{\pi'}(G)||H|}{|KO_{\pi'}(G) \cap H|} = \frac{|K||G|}{|K_1|},$$

于是 $|K_1| = |K|$. 这说明 K 和 K_1 是 $KO_{\pi'}(G)$ 的两个 π-Hall 子群. 由 Schur-Zassenhaus 定理, 存在 $x \in KO_{\pi'}(G)$ 使 $K^x = K_1 = KO_{\pi'}(G) \cap H$, 于是 $K^x \le H, K \le H^{x^{-1}}$. 定理得证. □

由本章末第 4 题, 定理 2.1 可以改述为

定理 2.1′ 设 G 是 π- 可解群, 则

(1) G 中存在 π-Hall 子群和 π'-Hall 子群;

(2) G 的所有 π-Hall 子群共轭, 并且 G 的所有 π'-Hall 子群也共轭;

(3) G 的任一 π- 子群包含在某一 π-Hall 子群之中. 对 π'- 子群也有类似结论.

推论 2.2 (P. Hall) 设 G 可解, 则对任一素数集合 π, G 中 π-Hall 子群存在并彼此共轭, 且任一 π- 子群含于某一 π-Hall 子群之中.

证　由 G 可解推出 G π- 可解, 应用定理 2.1′ 立得结论. □

定理 2.3 (P. Hall) 设 $|G| = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. 则 G 可解的充要条件为对于 $i = 1, \cdots, s$, G 中存在 p_i'-Hall 子群.

证　由推论 2.2 只须证明充分性. 我们用对 $|G|$ 的归纳法. 如果 $s = 1$, 即 G 是 p- 群, 当然可解. 如果 $s = 2$, 由定理 II,3.7(将在第 VI 章中证明), 亦可推出 G 可解. 故可设 $s \ge 3$, 并分下面两步来证:

1. 设 G 的 p_i'-Hall 子群是 H_i, 先证明 H_i 可解, $i = 1, \cdots, s$. 因为 $|G : H_i| = p_i^{\alpha_i}$, 故对 $i \ne j$ 有 $(|G : H_i|, |G : H_j|) = 1$. 由命题 I,1.19(3), 有 $|G : H_i \cap H_j| = p_i^{\alpha_i} p_j^{\alpha_j}$, 因此有 $|H_i : H_i \cap H_j| = p_j^{\alpha_j}$. 这说明 $H_i \cap H_j$ 是 H_i 的 p_j'-Hall 子群, 由归纳假设, 即得 H_i 的可解性.

2. 证明 G 可解: 考虑 G 的三个可解子群 H_1, H_2, H_3. 设对某个素数 p, 有 $M = O_p(H_1) \ne 1$. 因为 $(|G : H_2|, |G : H_3|) = 1$. p 至少整除 $|H_2|, |H_3|$ 中的一个. 不妨设 $p \mid |H_2|$, 并设 $P \le H_2$ 是 G 的

一个 Sylow p- 子群. 由 Sylow 定理, 存在 $g \in G$ 使 $M \le P^g \le H_2^g$. 再用命题 I,1.19(3), 有 $G = H_1H_2^g$. 故对任一元素 $x \in G$, 可设 $x = x_1x_2$, 其中 $x_1 \in H_1$, $x_2 \in H_2^g$. 由 $M \lhd H_1$, 且 $M \le H_2^g$, 有

$$M^x = M^{x_1x_2} = M^{x_2} \le H_2^g.$$

于是若令 $N = \langle M^x \mid x \in G\rangle$, 有 $N \le H_2^g$. 这样 $1 \ne N \lhd G$, 由 H_2^g 可解知 N 可解; 又因 H_iN/N 是 G/N 的 p_i'-Hall 子群, 由归纳假设得 G/N 的可解性. 最后便得到 G 的可解性. □

注 2.4 应用 2.3 的证明方法, 我们可以证明: 如果有限群 G 有三个指数两两互素的可解子群, 则 G 是可解的.

§3. Sylow 系和 Sylow 补系

定义 3.1 设 G 是可解群, $|G| = p_1^{\alpha_1}\cdots p_s^{\alpha_s}$. 再设 $G_{p_i} \in \mathrm{Syl}_{p_i}(G)$, $i = 1,\cdots,s$, 我们称 $\mathcal{S} = \{G_{p_1},\cdots,G_{p_s}\}$ 为 G 的一个 Sylow 系 (在有些文献上称为 Sylow 基), 如果对任意的 i,j 都满足 $G_{p_i}G_{p_j} = G_{p_j}G_{p_i}$. 又设 $G_{p_i'}$ 为 G 的任一个 p_i'- 子群, 我们称 $\mathcal{K} = \{G_{p_1'},\cdots,G_{p_s'}\}$ 为 G 的一个 Sylow 补系. 对于 Sylow 补系, 当然有 $G_{p_i'}G_{p_j'} = G_{p_j'}G_{p_i'}$, $i,j = 1,\cdots,s$.

定理 2.3 表明: G 可解的充要条件为 G 中存在 Sylow 补系 $\mathcal{K} = \{G_{p_1'},\cdots,G_{p_s'}\}$. 下面我们证明

定理 3.2 (P. Hall) G 可解的充要条件为 G 中存在 Sylow 系 $\mathcal{S} = \{G_{p_1},\cdots,G_{p_s}\}$.

证 $\Rightarrow$: 设 $|G| = p_1^{\alpha_1}\cdots p_s^{\alpha_s}$. 因 G 可解, G 中存在 Sylow 补系 $\mathcal{K} = \{G_{p_1'},\cdots,G_{p_s'}\}$. 我们将由 $\mathcal{K}$ 出发, 构造 G 的一个 Sylow 系. 首先, 我们注意到, 若 H 是 G 的任一 π-Hall 子群, $p_i \in \pi$, 则 $G_{p_i'} \cap H$ 是 G 的 $(\pi - \{p_i\})$-Hall 子群. 这是因为 $|G:H|$ 和 $|G:G_{p_i'}|$ 互素, 由命题 I,1.19 (3), 即得 $|G:G_{p_i'} \cap H| = |G:H||G:G_{p_i'}|$ 于

是 $G_{p_i'} \cap H$ 恰为 G 的一个 $(\pi - \{p_i\})$-Hall 子群. 由此我们便可得到 $\mathcal{K}$ 中任意多个子群的交都是 G 的 Hall- 子群. 于是, 若令 $G_{p_i} = \bigcap_{i \neq j} G_{p_j'}$, $i = 1, \cdots, s$, 则 G_{p_i} 是 G 的一个 Sylow p_i- 子群. 令 $\mathcal{S} = \{G_{p_1}, \cdots, G_{p_s}\}$, 我们断言 $\mathcal{S}$ 即为 G 的一个 Sylow 系, 即对任意的 i, j, 都有 $G_{p_i}G_{p_j} = G_{p_j}G_{p_i}$. 这因为 $G_{p_i}G_{p_j} \subseteq \bigcap_{k \neq i,j} G_{p_k'}$, 比较阶即得 $G_{p_i}G_{p_j} = \bigcap_{k \neq i,j} G_{p_k'}$. 同理又有 $G_{p_j}G_{p_i} = \bigcap_{k \neq i,j} G_{p_k'}$. 于是 $G_{p_i}G_{p_j} = G_{p_j}G_{p_i}$.

$\Leftarrow$: 设 $\mathcal{S} = \{G_{p_1}, \cdots, G_{p_s}\}$ 是群 G 的一个 Sylow 系, 则由 $G_{p_i}G_{p_j} = G_{p_j}G_{p_i}$, 对任意的 i, j 成立, 知 $G_{p_1} \cdots G_{p_{i-1}} G_{p_{i+1}} \cdots G_{p_s} = G_{p_i'}$ 是 G 的一个 p_i'-Hall 子群. 于是 G 存在 Sylow 补系, 由定理 2.3, G 可解. □

定理 3.3 (P. Hall) *设 G 是可解群, $\mathcal{K} = \{G_{p_1'}, \cdots, G_{p_s'}\}$ 和 $\mathcal{K}^* = \{G^*_{p_1'}, \cdots, G^*_{p_s'}\}$ 是 G 的任二 Sylow 补系, 则 $\mathcal{K}$ 和 $\mathcal{K}^*$ 共轭, 即存在 $g \in G$ 使对任意的 i 有 $G^g_{p_i'} = G^*_{p_i'}$.*

证 因为 G 可解, G 的任二 π-Hall 子群共轭. 于是对于 $i = 1, \cdots, s$, G 的 p_i'-Hall 子群的个数应为 $k_i = |G : N_G(G_{p_i'})|$, 它是 p_i 的方幂. 而 G 中不同的 Sylow 补系的个数应为 $k = \prod_{i=1}^{s} k_i$. 因为 $k_1, \cdots, k_s$ 两两互素, 据命题 I,1.19.(3),

$$k = \prod_{i=1}^{s} |G : N_G(G_{p_i'})| = |G : \bigcap_{i=1}^{s} N_G(G_{p_i'})|,$$

而后者恰为与 $\mathcal{K}$ 共轭的 Sylow 补系的个数, 由此推出 G 的任二 Sylow 补系共轭. □

推论 3.4 *可解群 G 的任二 Sylow 系亦共轭.*

证 只要注意到 G 的任一 Sylow 系可由某一 Sylow 补系取交得到, 由定理 3.3 即得所需的结果. □

§4. Fitting 子群

引理 4.1 设 G 是群, N_1, N_2 是 G 的幂零正规子群, 且 N_1 的幂零类 $c(N_1)=c_1$, N_2 的幂零类 $c(N_2)=c_2$, 则 N_1N_2 也是 G 的幂零正规子群, 而且 N_1N_2 的幂零类 $c(N_1N_2)\le c_1+c_2$.

证 容易验证, 若 A, B, C 皆为 G 之正规子群, 则有

$$[AB,C]=[A,C][B,C],$$

$$[A,BC]=[A,B][A,C].$$

(可参看第 IV 章习题的第 1 题.) 于是

$$(N_1N_2)_s=\underbrace{[N_1N_2,N_1N_2,\cdots,N_1N_2]}_{s\text{ 个}}$$

可表成 2^s 个形如 $[X_1,\cdots,X_s]$ 的因子的乘积, 其中 $X_i=N_1$ 或 N_2. 如果 $s\ge c_1+c_2+1$, 则在 $X_1,\cdots,X_s$ 中至少包含 c_1+1 个 N_1 或者 c_2+1 个 N_2. 注意到 $[M,N]\le M\cap N$, 只要 $M, N\trianglelefteq G$, 于是由 $c(N_1)=c_1$ 和 $c(N_2)=c_2$ 即可得到 $[X_1,\cdots,X_s]=1$, 于是 $(N_1N_2)_s=1$. 这就得到 N_1N_2 幂零, 且 $c(N_1N_2)\le c_1+c_2$. □

定义 4.2 设 G 是有限群, 则由引理 4.1, G 的所有幂零正规子群的乘积 $F(G)$ 仍为 G 之幂零正规子群, 叫做 G 的 Fitting **子群**.

Fitting 子群的简单性质是

定理 4.3 设 G 是有限群, $F(G)$ 是 G 的 Fitting 子群, $\Phi(G)$ 是 G 的 Frattini 子群. 则

(1) $\Phi(G)\le F(G)$, $F(G/\Phi(G))=F(G)/\Phi(G)$;

(2) 若 G 可解, $G\ne 1$, 则有 $F(G)\ne 1$, 进一步还有 $\Phi(G)<F(G)$;

(3) $C_G(F(G))F(G)/F(G)$ 不包含 $\ne 1$ 的可解正规子群. 特别地, 若 G 可解, 则 $C_G(F(G))\le F(G)$;

(4) 设 N 是 G 的极小正规子群, 则 $F(G)\le C_G(N)$. 特别, 若 N 是交换的, 则有 $N\le Z(F(G))$.

证 (1) 由 IV,3.8, $\Phi(G)$ 幂零. 又 $\Phi(G) \trianglelefteq G$, 于是 $\Phi(G) \le F(G)$. 设 $F(G/\Phi(G)) = N/\Phi(G)$. 据 IV,3.7, 由 $N/\Phi(G)$ 幂零可得 N 幂零，于是 $N \le F(G)$. 又由 $F(G)$ 幂零，有 $F(G)/\Phi(G)$ 幂零，故 $F(G)/\Phi(G) \le N/\Phi(G)$, $F(G) \le N$. 这样就得到 $N = F(G)$.

(2) 因 G 可解，$G \ne 1$, 由定理 1.7 知对某个素数 p 有 $O_p(G) \ne 1$. 显然 $O_p(G) \le F(G)$, 故 $F(G) \ne 1$.

令 $\overline{G} = G/\Phi(G)$, 亦有 $\overline{G}$ 可解且 $\overline{G} \ne 1$, 于是 $F(\overline{G}) \ne 1$. 由 (1), $F(G)/\Phi(G) \ne 1$, 即 $\Phi(G) < F(G)$.

(3) 令 $F = F(G)$, $C = C_G(F(G))$. 我们来证明 CF/F 没有 $\ne 1$ 的可解正规子群. 由 $CF/F \cong C/C \cap F = C/Z(F)$, 只须证 $C/Z(F)$ 没有 $\ne 1$ 的可解正规子群. 用反证法，若有，则对某个素数 p, 有 $O_p(C/Z(F)) \ne 1$. 令 $\overline{B} = B/Z(F) = Z(O_p(C/Z(F)))$, 则 $1 \ne \overline{B}$ 是交换群，于是 $B' \le Z(F)$. 又因 $B \le C = C_G(F(G))$, 故 $[Z(F), B] \le [Z(F), C] = 1$. 于是 $[B', B] = 1$, 这推出 B 幂零. 又由 B 的定义易证明 $B \trianglelefteq G$, 故 $B \le F$. 但是 $B \le C$, 故 $B \le C \cap F = Z(F)$, 于是 $\overline{B} = B/Z(F) = 1$, 矛盾.

(4) 设 N 是 G 的极小正规子群，则 $N \cap F(G) = 1$ 或 N. 若 $N \cap F(G) = 1$, 则 $[N, F(G)] \le N \cap F(G) = 1$, 于是 $F(G) \le C_G(N)$. 而若 $N \cap F(G) = N$, 即 $N \le F(G)$, 则由 $F(G)$ 幂零必有 $[F(G), N] < N$, 再由 $[F(G), N] \trianglelefteq G$ 及 N 的极小性有 $[F(G), N] = 1$, 亦得到 $F(G) \le C_G(N)$. □

下面的定理给出 Fitting 子群的一个刻画.

定理 4.4 *设 G 是有限群，$|G| = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. 则*

$$F(G) = O_{p_1}(G) \times \cdots \times O_{p_s}(G).$$

证 显然 $O_{p_1}(G) \times \cdots \times O_{p_s}(G)$ 幂零，于是 $O_{p_1}(G) \times \cdots \times O_{p_s}(G) \le F(G)$. 又设 N 是 G 的任一幂零正规子群，则 N 的 Sylow p_i- 子群 P_i char N, 于是 $P_i \trianglelefteq G$, 这就有 $P_i \le O_{p_i}(G)$. 又由 N 的幂零性有 $N = P_1 \times \cdots \times P_s$, 于是 $N \le O_{p_1}(G) \times \cdots \times O_{p_s}(G)$, 取 $N = F(G)$ 即得 $F(G) \le O_{p_1}(G) \times \cdots \times O_{p_s}(G)$. □

应用定理 4.4, 我们来证明 Fitting 子群的下述性质，它在可解群理论中经常要用到.

定理 4.5 设 G 是有限群，且 $\Phi(G)=1$, 则

(1) $O_p(G)$ 是初等交换 p- 群，且

$$O_p(G)=\langle N \mid N\text{是 } G \text{ 的极小正规子群，且 } N \text{ 是 } p\text{- 群}\rangle.$$

(2) $F(G)$ 是交换群，且

$$F(G)=\langle N \mid N\text{是 } G \text{ 的可解极小正规子群}\rangle.$$

证 (1) 若 $O_p(G)=1$, 则结论显然成立，故可设 $O_p(G)\neq 1$. 因 $O_p(G)\trianglelefteq G$, 由 IV,3.4, 有 $\Phi(O_p(G))\le\Phi(G)=1$. 再由 IV,5.1, $O_p(G)$ 是初等交换 p- 群.

设 N 是 G 的极小正规子群，且 N 为 p- 群，则由 $O_p(G)$ 的定义有 $N\le O_p(G)$. 于是若令

$$A=\langle N \mid N\text{是 } G \text{ 的极小正规子群，且 } N \text{ 是 } p\text{- 群}\rangle,$$

有 $A\le O_p(G)$.

为证明 $A=O_p(G)$, 我们先来证明 A 在 G 中有补，即存在 $B\le G$, 使 $AB=G$, $A\cap B=1$. 考虑集合

$$\mathcal{M}=\{M\le G \mid AM=G\}.$$

令 B 是 $\mathcal{M}$ 中一个极小元素. 我们证明 B 即为所求, 即成立 $A\cap B=1$. 若否，有 $C=A\cap B\neq 1$. 因 $A\trianglelefteq G$, 由同构定理， $C\trianglelefteq B$. 又因 A 交换，有 $C\trianglelefteq A$. 于是 $C\trianglelefteq AB=G$. 再由 $\Phi(G)=1$, 必存在 G 的极大子群 $S\not\geq C$, 于是 $SC=G$. 这时我们有

$$B=SC\cap B=C(S\cap B),$$

及

$$G=AB=AC(S\cap B)=A(S\cap B).$$

于是 $S\cap B\in\mathcal{M}$, 但 $S\cap B<B$, 与 B 的极小性矛盾. 这就证明了 A 在 G 中有补.

现在设 B 是 A 的一个补群. 令 $O_p(G)\cap B=D$, 则因 $O_p(G)$ 交换, 有 $D\trianglelefteq O_p(G)$. 又由同构定理, 有 $D\trianglelefteq B$, 于是 $D\trianglelefteq O_p(G)B=G$. 若 $D\neq 1$. 则在 D 中取 G 之极小正规子群 K, 有 $K\leq A$. 但 $K\leq B$, 故 $K\leq A\cap B=1$, 矛盾. 由此可知 $D=1$. 这时由 $G=O_p(G)B=AB$ 以及 $O_p(G)\cap B=A\cap B=1$, 比较阶得 $O_p(G)=A$.

(2) 因 G 的可解极小正规子群必为初等交换 p- 群, 由 (1) 及定理 4.4 立得结论. □

下面的推论是显然的.

推论 4.6 *设 G 为有限群, 则 $F(G)/\Phi(G)$ 为交换群, 且为 $G/\Phi(G)$ 之所有可解极小正规子群之乘积.*

定义 4.7 设 G 是有限群. 称 G 的所有极小正规子群的乘积为 G 的*基柱* (Socle), 记作 $\mathrm{Soc}(G)$.

由定理 4.5 和推论 4.6 立即可得

定理 4.8 *设 G 是有限可解群, 则 $F(G)/\Phi(G)=\mathrm{Soc}(G/\Phi(G))$. 特别地, 若 $\Phi(G)=1$, 则 $F(G)=\mathrm{Soc}(G)$, 且为 G 的极大交换正规子群.*

证 只须证 $F(G)=\mathrm{Soc}(G)$ 是 G 的极大交换正规子群, 若否, 将有 $C_G(F(G))>F(G)$, 与定理 4.3(3) 矛盾. □

上面用到: 对于有限可解群来说, 恒有 $C_G(F(G))\leq F(G)$, 即 $F(G)$ 是*自中心化的*. 这个性质在研究单群时十分有用. 但因为它对非可解群不一定成立, 故我们如下定义一个子群 $F^*(G)$, 叫做 G 的广义 Fitting 子群, 而它对任意有限群 G 都是自中心化的.

定义 4.9 设 G 是有限群, $F(G)$ 是 G 的 Fitting 子群. 令 $C=C_G(F(G))$, $Z=Z(F(G))$, 再令 $M/Z=\mathrm{Soc}(C/Z)$, 则称 $F^*(G)=MF(G)$ 为 G 之*广义 Fitting 子群*.

由于在此定义中出现的群均为 G 之特征子群, 故 $F^*(G)$ char G. 对于可解群 G, 由定理 4.3(3) 的证明, $\mathrm{Soc}(C/Z)=1$, 故 $F^*(G)=F(G)$. 因此我们称 $F^*(G)$ 为广义 Fitting 子群. 我们有

定理 4.10 $C_G(F^*(G))\leq F^*(G)$.

证 仍使用上面的符号, 再令 $C^*=C_G(F^*(G))$. 因为 $F(G)\leq F^*(G)$, 有 $C^*\leq C$, 且 C^* char C.

若 $C^*\not\leq F^*(G)$, 则 $C^*Z/Z\not\leq F^*(G)/Z=\mathrm{Soc}(C/Z)\cdot F(G)/Z$. 在 C^*Z/Z 中任取一 C/Z 之极小正规子群 N/Z, 由定理 4.3(3) 的证明, N/Z 是不可解的, 因而是非交换单群的直积. 但因 $C^*Z/Z\leq Z(F^*(G)/Z)$, 故 N/Z 是交换的, 矛盾. □

本章到此为止, 只是讲述了 π- 可分群, π- 可解群和可解群的最基本的知识以及研究可解群时经常用到的 Fitting 子群 $F(G)$. 关于可解群的进一步知识, 将在下册第 IX 章中讲述.

§5. Frobenius 定理

本章最后两节稍稍离开可解群的一般理论, 来讲述两个较古老的结果. 一个是本节讲的 Frobenius 定理, 特别要介绍一个著名的 Frobenius 猜想; 另一个是下节要讲的对 Sylow 子群皆循环的有限群的刻划.

定理 5.1 (Frobenius) *设 G 是群, $|G|=g$. C 是 G 的一个共轭元素类, $|C|=h$. 则当 c 跑遍 C 时, 方程 $x^n=c$ 在群 G 中解的个数是 (hn,g) 的倍数.*

证 对于 G 的任一子集 K, 令 $A(K,n)=\{x\in G\mid x^n\in K\}$, $a(K,n)=|A(K,n)|$. 本定理的结论即 (hn,g) 整除 $a(C,n)$. 我们用对 g 和 n 的双重归纳法来证明. 当 $g=1$ 或 $n=1$ 时结论显然. 现在设对 $|G_1|<g$ 或 $|G_1|=g$ 但 $n_1<n$ 的群 G_1 和 n_1 已经成立, 来考察对 G 和 n 的情况.

首先，若 $c' = u^{-1}cu$，则 $x^n = c \iff (u^{-1}xu)^n = c'$. 于是在方程 $x^n = c$ 和 $x^n = c'$ 的解集合间有一个一一对应，这推出 $a(C,n) = ha(c,n)$ 对任一 $c \in C$ 成立. 又，如果 $x^n = c$，则显然 $x \in C_G(c)$. 现在假定 $h > 1$，即 $|C_G(c)| = g/h < g$，对 $C_G(c)$ 应用归纳假设，有 $(n, g/h) \mid a(c,n)$，于是 $h(n, g/h)$ 可整除 $ha(a,n) = a(C,n)$，定理得证. 故下面可设 $h = 1$，这时有 $C = \{c\}$.

假定 $n = n_1n_2$，$(n_1, n_2) = 1$，$n_1 > 1$，$n_2 > 1$. 令 $D = A(c, n_2)$，则 $A(c,n) = A(D, n_1)$. 因为由 $x^{n_2} = c$ 可推出 $(a^{-1}xa)^{n_2} = a^{-1}ca = c$，$\forall a \in G$，故 D 为 G 的若干共轭类之并. 根据归纳假设，可推得 $(n_1, g) \mid a(c,n) = a(D, n_1)$. 同理，$(n_2, g) \mid a(c,n)$. 由 $(n_1, n_2) = 1$，即得 $(n, g) \mid a(c,n)$.

下面可设 $n = p^e$ 是素数方幂. 再分两种情形予以讨论：

(i) $p \mid o(c)$：这时对任意的 $x \in A(c,n)$，有 $o(x) = no(c)$. 于是在 $\langle x \rangle$ 中恰有 n 个元素属于 $A(c,n)$，即 x^i，其中 i 满足 $i \equiv 1 \pmod{o(c)}$ 者. 并且这 n 个元素生成同一循环子群 $\langle x \rangle$. 因此 $a(c,n)$ 是 n 的倍数，定理成立.

(ii) $p \nmid o(c)$：由 $h = 1$，有 $c \in Z(G)$. 因为 $Z(G)$ 是交换群，$Z(G)$ 中阶与 p 互素的元素组成子群 B，且 $p \nmid |B|$. 若有 $c_1, c_2 \in B$，则方程 $c_2 = c_1y^n$ 在 B 中有唯一解 y. 于是若 $x \in G$，$x^n = c_1$，则有 $(xy)^n = c_2$，反之亦然. 这推出 $a(c,n)$ 对于所有的 $c \in B$ 有相同的值，由 $G = \bigcup_C A(C,n)$，其中 C 跑遍 G 的所有共轭类，有

$$g = \sum_C a(C,n) = \sum_{C \not\subseteq B} a(C,n) + |B|a(c,n).$$

因为 (n,g) 可整除第一和式中的每一项，故亦可整除 $|B|a(c,n)$，由 $(n, |B|) = 1$，即得 $(n,g) \mid a(c,n)$. □

推论 5.2 *若 $n \mid |G|$，则方程 $x^n = 1$ 在 G 中的解的个数是 n 的倍数.*

与此相关的有 Frobenius 的著名猜想：若 $n \mid |G|$，且 $x^n = 1$ 在 G 中恰在 n 个解，则它们组成 G 的正规子群. 这个猜想至今

尚未得到证明.[1] 但对于可解群，我们有

定理 5.3 设 G 是 g 阶可解群，$n \mid g$, 且方程 $x^n = 1$ 在 G 中恰有 n 个解，则它们组成 G 的正规子群.

证 对 g 用归纳法，取 G 的极小正规子群 N, 令 $\overline{G} = G/N$, 因为 G 可解，N 是 p^i 阶初等交换 p- 群，分下面两种情形予以讨论：

(i) $p \mid n$: 这时 N 中元素皆满足方程 $x^n = 1$. 设 $n = p^j n_1$, $(p, n_1) = 1$; $g = p^s g_1$, $(p, g_1) = 1$, 有 $|\overline{G}| = p^{s-i} g_1$. 令

$$n' = \begin{cases} p^{j-i} n_1, & \text{当} j \geq i, \\ n_1, & \text{当} j < i. \end{cases}$$

则显然 $n' \mid |\overline{G}|$, 于是 $\overline{x}^{n'} = 1$ 在 $\overline{G}$ 中有 kn' 个解，并且每个解 $\overline{x} = xN$(作为 N 的陪集) 中的任一元素 xa, 其中 $a \in N$, 满足 G 中方程 $(xa)^{n'p} = 1$, 因而 $(xa)^n = 1$. 这推出 G 中方程 $x^n = 1$ 至少有 $kn'p^i$ 个解. 若 $j < i$, $n'p^i > n$, 与 $x^n = 1$ 恰有 n 个解相矛盾. 故必有 $j \geq i$, 且 $k = 1$. 由此，方程 $\overline{x}^{n'} = 1$ 在 $\overline{G}$ 中也恰有 n' 个解. 据归纳假设，这些解组成 $\overline{G}$ 的 n' 阶正规子群 K/N, 于是 K 是 G 的 n 阶正规子群.

(ii) $p \nmid n$: 这时在 $\overline{G}$ 中 $\overline{x}^n = 1$ 有 kn 个解. 对于任一解 $\overline{x} = xN$, 考察 $H = \langle x, N \rangle$. 因为 $(|N|, |H:N|) = 1$, 在 xN 中存在一个元素 xa, $a \in N$, 使 $o(xa) = o(\overline{x}) = |H:N|$, 于是 $(xa)^n = 1$. 这样在 G 中，方程 $x^n = 1$ 至少有 kn 个解. 由已知条件 $k = 1$, 即方程 $\overline{x}^n = 1$ 在 $\overline{G}$ 中也恰有 n 个解. 依归纳假设，这 n 个解组成正规子群 K/N, 其中 $|K| = np$. 由 K 可解 (或用 Schur-Zassenhaus 定理), K 中存在 p'-Hall 子群 K_1, 有 $|K_1| = n$. 于是 K_1 恰由 G 中方程 $x^n = 1$ 的 n 个解所组成，是 G 的 n 阶正规子群. □

---

[1] 目前这个猜想已经得到证明，可见 N. Iiyori 和 H. Yamaki 的文章 "On a conjecture of Frobenius," 载 Bull. Amer. Math. Soc., vol. 25(1991), 413–416.

§6. 所有 Sylow 子群皆循环的有限群

为决定所有有限群的构造，人们尝试了两种不同的途径．第一种是第 III 章中介绍的先决定有限单群，再应用群扩张理论由给定的合成因子决定群的方法，这方面目前已取得了较大的成就．第二种是企图先决定所有的有限 p- 群，然后设法造出以给定的 p- 群为 Sylow 子群的有限群．这种企图目前还很少成功．这一方面是因为 p- 群构造的复杂性，决定所有有限 p- 群的任务是十分困难的；另外也因为 Sylow 子群对整个群构造的影响目前还知之甚少．但是这方面还是有些成功的例证的．本节的目的是决定所有 Sylow 子群皆循环的有限群，这可以作为依第二种途径构造有限群的一个最简单的但也是成功的例子．

引理 6.1 *设 G 是群．若 G'/G'' 和 G''/G''' 都是循环群，则 $G''=G'''$.*

证　若假定 $G'''=1$ 能推出 $G''=1$ 即可完成证明．这时 G'' 循环，可令 $G''=\langle b\rangle$．由 N/C 定理，$G/C_G(G'')$ 同构于 $\mathrm{Aut}(G'')=\mathrm{Aut}(\langle b\rangle)$ 的子群，因而是交换群．于是 $C_G(G'')\geq G'$，$G''\leq Z(G')$．又因 G'/G'' 循环，得 G' 交换，于是 $G''=1$.　□

定理 6.2 *设有限群 G 的所有 Sylow 子群皆为循环群．若 G 交换，则 G 为循环群；而若 G 非交换，则 G 为由下列定义关系确定的亚循环群：*

$$G=\langle a,b\rangle, a^m=b^n=1, b^{-1}ab=a^r,$$

$$((r-1)n,m)=1, r^n\equiv 1 \pmod m), |G|=nm.$$

证　首先，G 必为可解群，这点由 II, 推论 5.6 已经得到．现在再给一个新证明．设 $|G|=p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$, $p_1<p_2<\cdots<p_s$．我们证明对于 $m=p_j^{b_j}p_{j+1}^{a_{j+1}}\cdots p_s^{a_s}$, $b_j\leq a_i$, $1\leq j\leq s$, 方程 $x^m=1$ 在 G 中恰有 m 个解．应用反向归纳法．首先，当 $m=|G|$ 时结论显然成立．因此只要证明，如果 $x^{mp}=1$ 在 G 中恰有 mp 个解，其中

p 是 mp 的最小素因子，则 $x^m=1$ 在 G 中也恰有 m 个解. 设 p^{b+1} 是整数 pm 的 p 的最高次幂. 因为 G 的 Sylow p- 子群循环，G 中存在 p^{b+1} 阶元素，它们是 $x^{mp}=1$ 的解，但不是 $x^m=1$ 的解，于是 $x^m=1$ 的解的个数应为 km 个，其中 $1\le k<p$. 设 y 是满足 $x^{mp}=1$ 但不满足 $x^m=1$ 的一个元素，则 $p^{b+1}\mid o(y)$. 于是在 $\langle y\rangle$ 中 $\varphi(o(y))$ 个生成元也都是 $x^{mp}=1$ 的解，但不是 $x^m=1$ 的解，它们生成同一个循环子群 $\langle y\rangle$. 因为 $p\mid o(y)$, 故 $(p-1)\mid\varphi(o(y))$, 这推出 $p-1$ 能整除满足 $x^{mp}=1$ 但不满足 $x^m=1$ 的元素的个数 $pm-km=(p-k)m$. 又因 p 是整除 mp 的最小素因子，有 $p-1=p-k$. 于是 $k=1$, 即 $x^m=1$ 在 G 中也恰有 m 个解. 现在令 $m=p_s^{a_s}$. 由 $x^m=1$ 在 G 中恰有 m 个解以及 m 阶子群即 Sylow p_s- 子群的存在性，推知 G 的 Sylow p_s- 子群 $P_s\trianglelefteq G$. 而商群 $\overline{G}=G/P_s$ 的诸 Sylow 子群仍循环. 于是由归纳法即可得到 $\overline{G}$, 从而得到 G 的可解性.

下面除去 G 交换的简单情形来证明 G 有所给的定义关系. 因为 Sylow 子群皆循环的交换群是循环群，故 $G/G', G'/G'', \cdots$ 都是循环群. 应用引理 6.1 有 $G''=G'''$. 又因为 G 可解，必有 $G''=1$. 这样 G' 和 G/G' 都是循环群. 令 $G'=\langle a\rangle$ 是 m 阶循环群，$G/G'=\langle bG'\rangle$ 是 n 阶循环群，则由 $G'\trianglelefteq G$, 有 $b^{-1}ab=a^r$, $r\not\equiv 1 \pmod m$. 但因 $b^n\in\langle a\rangle$ 及 $b^{-n}ab^n=a^{r^n}$, 又有 $r^n\equiv 1 \pmod m$. 再由 G' 循环，得 $G'=\langle [a,b]\rangle=\langle a^{r-1}\rangle$. 而 $G'=\langle a\rangle$, 故 $(r-1,m)=1$. 现在令 $b^n=a^j$, 有 $b^{-1}a^jb=a^j$, 即 $a^{rj}=a^j$, $a^{(r-1)j}=1$. 由 $(r-1,m)=1$, 有 $a^j=1$, 即 $b^n=1$. 最后我们断言 $(n,m)=1$. 这因为若 $p\mid(n,m)$, 则 $\langle a^{m/p},b^{n/p}\rangle$ 是 p^2 阶初等交换 p- 群，与 G 的 Sylow p- 子群循环相矛盾，这就证明了 G 具有定理所给的定义关系.

最后，若 G 有定理所给的定义关系，则由循环扩张的理论知 $G=\mathrm{Ext}(\langle a\rangle;n,1,\sigma)$, 其中 σ 是 $\langle a\rangle$ 的自同构，满足 $a^\sigma=a^r$. 显然这时 G 的 Sylow 子群皆为循环群. □

推论 6.3 *若有限群 G 的阶不含平方因子，则 G 可解，并为上定理中描述的亚循环群.*

证 显然这时 G 的每个 Sylow 子群皆为循环群. 由定理 6.2 立得结论. □

习 题

1. 可解群必有一个极大子群是正规子群.

2. 设 M 是 π- 可分群 G 的极大子群, 则 $|G:M|$ 的素因子全在 π 内或全在 π' 内.

3. 设 G 是有限群, $H \le G$. 如果对任意的 $x \in H$, $x \neq 1$, 都有 $C_G(x) \le H$, 我们称 H 为 G 的一个 CC 子群. 证明 CC 子群必为 Hall 子群.

4. 设 G 是 π- 可分群. 则 G π- 可解的充要条件为 G 的任一 π-Hall 子群是可解群.

5. 设 P 是 G 的一个 Sylow p- 子群, A 是 P 的极大交换正规子群. 则

$$C_G(A) = A \times O_{p'}(C_G(A)).$$

6. 设 G 是 π- 可分群, 若 $O_{\pi'}(G) = 1$, 则 $C_G(O_\pi(G)) \le O_\pi(G)$.

7. 设 G 是 π- 可分群, K 是 $O_{\pi'}(G)$ 在 $O_{\pi'\pi}(G)$ 中的补群. 则 $C_G(K) \le O_{\pi'\pi}(G)$.

8. 设 G 是 p- 可解群, 且 $O_{p'}(G) = 1$. 令 $V = O_p(G)/\Phi(O_p(G))$. 对于任意的 $x \in G$, 规定 $\varphi(x) \in \mathrm{Aut}(V)$:

$$v^{\varphi(x)} = v^{\overline{x}}, \forall v \in V$$

其中 $\overline{x} = x\Phi(O_p(G))$. 则 φ 是 G 到 $\mathrm{Aut}(V)$ 内的同态, 其核 $\mathrm{Ker}\ \varphi = O_p(G)$.

9. 设 G 是 p- 可解群, 且 $O_{p'}(G) = 1$. 令 $P \in \mathrm{Syl}_p(G)$, 则

(1) 若 P 交换, 则 $P = O_p(G)$;

(2) $Z(P) \le Z(O_p(G))$;

(3) $Z(P)$ 的正规闭包 $Z(P)^G$ 是 G 的交换正规子群;

(4) 若 $O_p(G)$ 循环, 则 $G' \le O_p(G)$;

(5) 又设 $p = 2$, 若 P 循环或为阶 ≥ 16 的二面体群, 则 $P = G$; 若 P 是阶 ≤ 8 的二面体群, 则 G 同构于 S_4 的一个子群, 若 P 是 8 阶四元数群, 则 $G = O_{pp'}(G)$.

10. 试不用 Schur-Zassenhaus 定理证明可解群 G 中 p- 补群的存在性.

11. 设 G 是有限群, π 是一个素数集合. 如果 G 的每个主因子的阶至多可被 π 中一个素数整除, 则 G 有可解 π-Hall 子群, 并且所有 π-Hall 子群在 G 中共轭.

12. 设 G 是有限可解群， $H \le G$. 则对于 H 的每个 Sylow 系 $\mathcal{S}_H = \{H_p \mid p \text{ 整除 } |H|\}$, 存在 G 的一个 Sylow 系 $\mathcal{S}_G\{G_p \mid p \text{ 整除 } |G|\}$, 使 $H_p = G_p \cap H$ 对任意的 p 成立.

13. 设 G 是有限可解群， $N \trianglelefteq G$. 若 $\{G_p \mid p \text{ 整除 } |G|\}$ 是 G 的一个 Sylow 系，则 $\{N \cap G_p \mid p \text{ 整除 } |N|\}$ 是 N 的一个 Sylow 系.

14. 设 G 可解, H 是 G 的 π-Hall 子群, $K \ge N_G(H)$, 则 $N_G(K) = K$, 又若 $N \trianglelefteq G$, 则 $N_{G/H}(HN/N) = N_G(H)N/N$.

15. 设 G 是有限群， $F(G)$ 是 p- 群，则 $F(G/F(G))$ 是 p'- 群.

16. 设 G 可解， $\Phi(G) = 1$, 且 G 中只有唯一的极小正规子群 N, 则 $F(G) = N$.

17. 设 G 是有限群， $\Phi(G) = 1$. 则 $F(G)$ 是 G 中唯一的极大交换正规子群.

18. 设 G 是有限群， $12 \mid |G|$, 且 $x^{12} = 1$ 在 G 中恰有 12 个解，则这些解组成 G 的正规子群.

第 VI 章

有限群表示论初步

群表示论是群论的一个重要分支，它对群论本身以及对物理、化学等其它学科有着广泛的应用，它是上世纪末由 G. Frobenius 所创立，其时 W. Burnside 等人也作出了很大的贡献. 到了本世纪初，所谓*常表示*(ordinary representation) 的理论可以认为已经完成. 那时， Burnside 和 Frobenius 证明了两个著名的定理，使人们看到群表示，特别是群特征标的理论对于有限群论来说是何等重要！从本世纪 30 年代开始， R. Brauer 等人又进而发展了所谓*模表示*(modular representation) 的理论，它对于有限群论特别是有限单群的分类问题又提供了一个有力的工具.

在本章中，我们在叙述了群表示的若干基本概念之后，只局限于介绍常表示和常特征标的一些基本知识以及它们的若干应用.

本章中，恒假定 $\mathbf{F}$ 是一个域， G 是一个有限群，且 $|G| = g$.

§1. 群的表示

本节中假定 $V = V(n, \mathbf{F})$ 是 $\mathbf{F}$ 上的 n 维向量空间，并以 $GL(V)$ 表示 V 的全体可逆线性变换组成的乘法群，而以 $GL(n, \mathbf{F})$ 表示 $\mathbf{F}$ 上全体 $n \times n$ 可逆矩阵组成的乘法群. 当然二者是同构的.

定义 1.1 称群 G 到 $GL(V)$ 内的一个同态映射 X 为 G 的一个(线性) 表示，并称 $\mathbf{F}$ 为表示的*基域*，V 叫表示空间，而 $\dim V = n$ 叫做表示的*级*.

又称群 G 到 $GL(n,\mathbf{F})$ 内的一个同态映射 $\mathbf{X}$ 为 G 的一个 (矩阵) 表示. 同样, $\mathbf{F}$ 也叫做表示的基域, 而矩阵的阶 n 叫做表示的级.

设给定群 G 的一个线性表示 X. 在表示空间 V 内取一组基 $e_1,\cdots,e_n$. 对于任意的 $a\in G$, $X(a)$ 是 V 的一个线性变换. 令

$$e_i^{X(a)}=\sum_{j=1}^{n}a_{ij}(a)e_j. \tag{1.1}$$

于是得到对应于 $X(a)$ 的矩阵 $\mathbf{X}(a)=(a_{ij}(a))$, 并且 $a\mapsto\mathbf{X}(a)$ 是 G 的一个矩阵表示. 反过来, 由一个矩阵表示 $\mathbf{X}$ 出发, 取 V 为 $\mathbf{F}$ 上任一 n 维向量空间, $e_1,\cdots,e_n$ 是 V 的一组基. 则 (1.1) 式也确定了 G 的一个线性变换, 并且映射 $a\mapsto X(a)$ 是 G 到 $GL(V)$ 内的一个线性表示. 由此看来, 线性表示和矩阵表示本质上是一致的, 它们只有形式上的不同, 因此, 以后我们谈群的表示时, 就不再特别区分是矩阵表示还是线性表示, 而视所讨论的问题的需要, 哪种更方便就采用哪种形式, 在以下诸定义的叙述中, 我们基本上只对线性表示来进行, 而矩阵表示的相应定义请读者自行补足.

定义 1.2 设 $X:G\to GL(V)$ 是一个表示. 称同态核 Ker X 为*表示 X 的核*, 显然 Ker $X\trianglelefteq G$. 如果 Ker $X=G$, 则称 X 为 G 的*平凡表示*. 如果 Ker $X=1$, 则称 X 为 G 的一个*忠实表示*.

定义 1.3 设 $X_1:G\to GL(V_1)$ 和 $X_2:G\to GL(V_2)$ 是 G 的两个表示, 我们称*表示 X_1 和 X_2 等价*, 记作 $X_1\sim X_2$, 如果存在向量空间的同构 $S:V_1\to V_2$, 使

$$X_1(a)S=SX_2(a),\ \forall a\in G.$$

我们通常称这个事实为下面的图是交换的:

$$\begin{array}{ccc} V_1 & \xrightarrow{S} & V_2 \\ \downarrow{\scriptstyle X_1(a)} & & \downarrow{\scriptstyle X_2(a)} \\ V_1 & \xrightarrow{S} & V_2 \end{array}$$

显然，等价表示的级必然相等.

读者容易看出，矩阵表示 $\mathbf{X}_1$ 和 $\mathbf{X}_2$ 的等价可定义为存在满秩矩阵 S 使

$$\mathbf{S}^{-1}\mathbf{X}_1(a)\mathbf{S} = \mathbf{X}_2(a), \ \forall a \in G.$$

因此，等价的矩阵表示可以看作是同一个线性表示在不同的基之下的矩阵形式. 反过来，等价的线性表示在适当选取的二表示空间的基之下可以有相同的矩阵形式. 由于这个理由，在表示论中，我们常把等价的表示看作是同样的.

定义 1.4 设 $X : G \to GL(V)$ 是群 G 的一个表示. 规定群 G 在 V 上的作用如下：

$$v^a = v^{X(a)}, \ \forall v \in V, \ a \in G.$$

它满足

$$v^{ab} = (v^a)^b, \ \forall a, b \in G, \ v \in V.$$

我们称这个规定了群 G 的作用的线性空间 V 为一个 G-空间.

显然，给出一个表示 X 和给出一个 G-空间 V 是一回事. 因此，对群 G 的表示的研究可以看成是对 G-空间的研究.

定义 1.5 设 V 是一个 G-空间，W 是 V(作为线性空间) 的一个子空间. 如果 W 在 G 的作用下封闭，即满足

$$w^a \in W, \ \forall w \in W, \ a \in G,$$

则称 W 为 V 的一个 G-子空间.

明显地，$\{0\}$ 和 V 都是 V 的 G-子空间，叫做 V 的平凡 G-子空间.

设 W 是 G-空间 V 的非平凡 G-子空间. 则把 $X(a)$ 限制在 W 上亦为 W 的一个线性变换 $X(a)|_W$, 并且映射

$$Y : a \mapsto X(a)|_W,\ \forall a \in G,$$

也是 G 的表示，叫做由 X 在 W 上诱导的表示. 它的表示空间是 W.

我们再考虑商空间 V/W. 若规定

$$(v+W)^a = v^a + W,\ \forall v \in V, a \in G,$$

则可使商空间 V/W 亦成一 G-空间, 它所对应的表示设为 $Z : G \to GL(V/W)$.

如果在 V 中取一组基 $e_1, \cdots, e_m, \cdots, e_n$, 使 $e_1, \cdots, e_m$ 为 W 的基，于是 $e_{m+1}+W, \cdots, e_n+W$ 就是 V/W 的一组基. 这时 $X(a)$ 在这组基之下所对应的矩阵 $\mathbf{X}(a)$ 应有下列形状：

$$\mathbf{X}(a) = \begin{pmatrix} \mathbf{Y}(a) & 0 \\ * & \mathbf{Z}(a) \end{pmatrix},$$

其中 $\mathbf{Y}, \mathbf{Z}$ 分别为表示 Y, Z 对应的矩阵，而 0 是 m 行，$(n-m)$ 列的零矩阵.

定义 1.6 设 $X : G \to GL(V)$ 是群 G 的表示， V 是相应的 G-空间，如果 V 中存在一个非平凡 G-子空间 W, 则称表示 X 以及 G-空间 V 为 **可约的**, 否则称为 **不可约的**. 而如果 V 可表成它的两个非平凡 G-子空间 W 和 W' 的直和： $V = W \oplus W'$, 则称表示 X 以及 G-空间 V 为 **可分解的**, 否则称为 **不可分解的**. 又，如果 V 可表成若干个不可约 G-子空间 W_i 的直和：

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_k,$$

则称表示 X 以及 G-空间 V 为 **完全可约的**.

假定 V 是可分解的，设 $V=W\oplus W'$. 我们在 W 和 W' 中各取一组基，并把它们合并成 V 的一组基. 则 $X(a)$ 在这组基下的矩阵 $\mathbf{X}(a)$ 有形状

$$\mathbf{X}(a)=\begin{pmatrix}\mathbf{Y}(a) & 0\\ 0 & \mathbf{Z}(a)\end{pmatrix}.$$

在这种情况下，我们也称表示 X 为前面规定的表示 Y 和 Z 的直和，记作 $X=Y\oplus Z$.

把 G 的每个元素都映到数 1 (看作 $\mathbf{F}$ 上的一阶方阵) 的映射显然是 G 的一个表示，叫做 G 的 *1-表示* 或 *主表示*, 常常记作 1_G. 它是任何群都有的一个 1 级表示，它当然是不可约的，但通常不是忠实的.

下面我们举几个较复杂的群表示的例子.

例 1.7 设群 G 作用在集合 $\Omega=\{1,\cdots,n\}$ 上. 对于任意的 $a\in G$, 令 $\mathbf{P}(a)=(a_{ij})_{n\times n}$, 其中

$$a_{ij}=\begin{cases}1, & 若 i^a=j,\\ 0, & 其它情形.\end{cases}$$

则映射 $\mathbf{P}:a\mapsto\mathbf{P}(a)$ 是 G 的一个 n 级矩阵表示，叫做 G 在 Ω 上的一个 *置换表示*. 这时，每个 $\mathbf{P}(a)$ 都是所谓 *置换矩阵*, 即每行每列都有一个 1, 而其余地方为 0 的矩阵. 置换表示 $\mathbf{P}$ 的核即群 G 在 Ω 上作用的核.

例 1.8 设 $G=\{1=a_1,a_2,\cdots,a_g\}$. 对于每个 $a\in G$, 令 $\mathbf{R}(a)=(a_{ij})_{g\times g}$, 其中

$$a_{ij}=\begin{cases}1, & 若 a_ia=a_j,\\ 0, & 其它情形.\end{cases}$$

则映射 $\mathbf{R}:a\mapsto\mathbf{R}(a)$ 是 G 的一个表示，叫做 G 的 *(右) 正则表示*.

正则表示是例 1.7 中给出的置换表示的特例，这时 G 所作用的集合就是 G 本身，正则表示在群表示论中起着很重要的作用.

明显地，正则表示一定是忠实表示.

例 1.9 设 $G \neq 1$ 是有限 p-可解群，且 $O_{p'}(G) = 1$. 则这时必有 $O_p(G) \neq 1$. 令 $V = O_p(G)/\Phi(O_p(G))$, 则 V 可看成 $GF(p)$ 上的有限维向量空间. 对于任一元素 $a \in G$, 在共轭作用下它诱导出 $O_p(G)$ 的一个自同构，从而也诱导出 V 的一个自同构，即线性变换. 这样可把 V 看成 G-空间，得到 G 的一个线性表示 $X : G \to GL(V)$. 由第 V 章习题 8 知， $\mathrm{Ker}\, X = O_p(G)$. 于是 X 可看成 $G/O_p(G)$ 的一个忠实表示.

这个例子在 Hall-Higman p-长理论中占有重要的地位.

命题 1.10 *设 G 是 p-群， $X : G \to GL(V)$ 是 G 在特征 p 域 $\mathbf{F}$ 上的不可约表示. 则 X 必为平凡表示，即 $\mathrm{Ker}\, X = G$ 且 $\dim_{\mathbf{F}} V = 1$.*

证 我们只需证明在 V 中存在非零向量 v 使 $v^{X(a)} = v, \forall a \in G$. 因为证明了这点，所有满足上述性质的向量必组成 V 的一个非零 G-子空间. 由 V 的不可约性，这个子空间必为 V 本身，于是有 $\mathrm{Ker}\, X = G$. 再由 V 的不可约性，必有 $\dim_{\mathbf{F}} V = 1$. 下面我们用对 $|G|$ 的归纳法证明 V 中存在在所有的 $X(a)$ 之下都不变的非零向量.

取 G 的任一极大子群 M, 因 G 是 p-群，有 $M \lhd G$. 由归纳假设，在 M 的作用之下保持不动的向量全体组成 V 的非零子空间，设其为 W. 我们先来证明 W 也是 G-子空间，即在 G 的作用之下不变. 为此，设 $a \in G, w \in W$, 我们要证明的是 $w^{X(a)} \in W$, 即证明 $w^{X(a)X(m)} = w^{X(a)}, \forall m \in M$. 因为 $M \lhd G$, 存在 $m' \in M$ 使 $am = m'a$, 于是

$$\begin{aligned} w^{X(a)X(m)} &= w^{X(am)} = w^{X(m'a)} \\ &= w^{X(m')X(a)} = w^{X(a)} , \end{aligned}$$

得证. 这样 W 是 V 的 G-子空间. 根据 V 的不可约性就推出 $W = V$, 即 M 在 V 上的作用是平凡的. 下面任取 $a \in G$ 但 $a \notin M$, 则有 $a^p \in M$. 于是 $X(a^p) = 1$, 即 $X(a)^p = 1$, 这里 1 是 V 的恒

等变换. 因为 char $\mathbf{F} = p$, 又推出 $(X(a)-1)^p = 0$, 即 $X(a)$ 满足方程 $(x-1)^p = 0$. 于是得到 1 是 $X(a)$ 的一个 (也是仅有的) 特征根. 取 $v \neq 0$ 为 $X(a)$ 关于特征根 1 的特征向量, 这样 $v^{X(a)} = v$. 又因 v 在 M 下不变, 故 v 在 $\langle M, a\rangle = G$ 下不变. 命题得证. □

推论 1.11 *设群 G 在特征为 p 的域 $\mathbf{F}$ 上有一不可约忠实表示, 则 $O_p(G) = 1$.*

证 设 W 为被 $O_p(G)$ 不变的向量全体组成的子空间, 由命题 1.10 知 $W \neq 0$. 因为 $O_p(G) \lhd G$, 和命题 1.10 的证明一样, 我们可推出 W 也是 V 的 G-子空间. 于是由 V 的不可约性必有 $W = V$, 即 $O_p(G)$ 在 V 上作用是平凡的. 又因 G 的作用是忠实的, 就得到 $O_p(G) = 1$. □

到现在为止, 我们讨论的表示的基域 $\mathbf{F}$ 都是任意的. 但在进一步研究群表示的时候, 我们将看到对基域 $\mathbf{F}$ 加上某些限制是方便的. 比如, 设 $a \in G$, $o(a) = n$. 于是在任一表示 X 之下, $X(a)$ 满足 $(X(a))^n = 1$, 这里 1 是恒等变换. 这说明, 作为线性变换, $X(a)$ 的特征根都是域 $\mathbf{F}$ 中的 n 次单位根. 如果假设域 $\mathbf{F}$ 包含 n 次单位根, 显然对问题的讨论将带来很大方便. 通常为了简单起见, 我们甚至假定域 $\mathbf{F}$ 是代数封闭的, 这将使问题大大简化. 实际上, 域 $\mathbf{F}$ 的性质对群的表示影响是很大的. 一个 $\mathbf{F}$ 上的不可约表示, 当基域扩大了, 就可能变为可约的. 于是, 我们引进下述概念:

定义 1.12 设 X 是群 G 在域 $\mathbf{F}$ 上的不可约表示, 如果无论基域 $\mathbf{F}$ 怎样扩大, X 都仍为不可约的. 则称 X 为群 G 在域 $\mathbf{F}$ 上的 *绝对不可约表示*.

定义 1.13 如果群 G 在域 $\mathbf{F}$ 上的所有不可约表示为绝对不可约的, 则称 $\mathbf{F}$ 为 G 的 *分裂域*.

关于分裂域的进一步讨论超出了本书的范围, 有兴趣的读者可参看群表示论的更详尽的教科书.

为了熟悉群表示的基本概念，在本节的最后，我们来研究有限交换群的表示，尽管其中的主要结论都可由后面的群表示的一般理论推出. 首先证明两个较一般性的结果.

命题 1.14 *设 G 是群，不一定交换，而 z 是 G 的中心 $Z(G)$ 中的任一元素. 设 $|G|=g$, 且域 $\mathbf{F}$ 包含 g 次本原单位根. 又设 $X:G\to GL(V)$ 是 G 在 $\mathbf{F}$ 上一个不可约表示. 则 $X(z)$ 必为数乘变换，即对某 $\lambda\in\mathbf{F}$ 有 $v^{X(z)}=\lambda v$, $\forall v\in V$.*

证 因为 $\mathbf{F}$ 包含 g 次本原单位根，且 $(X(z))^g=1$, $X(z)$ 在 $\mathbf{F}$ 中存在特征根. 设其中的一个为 λ, 且 W 是 $X(z)$ 属于 λ 的特征子空间. 我们要证明 W 必为 V(作为 G-空间) 的一个 G-子空间. 这只须证对任意的 $a\in G$, $w\in W$, 有 $w^{X(a)}\in W$. 因为

$$(w^{X(a)})^{X(z)}=w^{X(az)}=w^{X(za)}=(w^{X(z)})^{X(a)}=\lambda w^{X(a)},$$

知 $w^{X(a)}$ 仍为 $X(z)$ 的属于 λ 的特征向量，于是 $w^{X(a)}\in W$, 由 V 的不可约性以及 $W\neq\{0\}$ 推知 $W=V$, 即 $X(z)$ 是 V 的数乘变换. □

推论 1.15 *在命题 1.14 中补充假定 X 是忠实表示，则 $Z(G)$ 是循环群.*

证 由命题 1.14, 对任一 $z\in Z(G)$, 有 $X(z)=\lambda\cdot 1$, 其中 1 表 V 的恒等映射. 设 $|G|=g$, 必有 $z^g=1$, 于是 $X(z)^g=\lambda^g\cdot 1=1$. 由此有 $\lambda^g=1$, 特别地，$\lambda\neq 0$, 即 $\lambda\in\mathbf{F}^{\#}$. 容易验证把 z 映到 λ 的映射是 $Z(G)$ 到群 $(\mathbf{F}^{\#},\cdot)$ 内的同态. 因为 $(\mathbf{F}^{\#},\cdot)$ 的有限子群为循环群，由 X 的忠实性即得到 $Z(G)$ 循环. □

下面开始分析交换群的表示.

定理 1.16 *设 G 是有限交换群，$|G|=g$, 且域 $\mathbf{F}$ 包含 g 次本原单位根. 设 $X:G\to GL(V)$ 是 G 的不可约表示，则 $\dim_{\mathbf{F}}V=1$, 即 X 为 1 级表示.*

证 由 G 交换，有 $G = Z(G)$. 命题 1.14 说明，对任意的 $0 \neq v \in V$ 有 $\langle v \rangle$ 是 V 的 G-子空间. 由 V 不可约及 $\langle v \rangle \neq \{0\}$, 即得 $V = \langle v \rangle$, 即 $\dim_{\mathbf{F}} V = 1$. □

下面研究交换群的 1 级表示. 根据交换群的分解定理，每个有限交换群都可表成有限多个循环群的直积. 故我们先来研究循环群的表示.

定理 1.17 设 $G = \langle a \rangle$ 是 n 阶循环群，域 $\mathbf{F}$ 包含 n 次本原单位根 ω. 且设 $\operatorname{char} \mathbf{F} = 0$ 或 p, $(p, n) = 1$. 则 G 恰有 n 个不可约表示 $X_1, \cdots, X_n$, 它们由下式确定：

$$X_i(a) = \omega^i, \quad i = 1, \cdots, n.$$

证 设 X 是 G 的一个不可约表示. 由定理 1.16, X 必为 1 级的. 如果我们不区别一维空间 V 的数乘变换 $\lambda \cdot 1$ 和数 λ, 可令 $X(a) = \lambda$, 其中 $\lambda \in \mathbf{F}^{\#}$. 因 $a^n = 1$, 故 $X(a)^n = 1$, 即 $\lambda^n = 1$. 所以 λ 是 n 次单位根. 即 $\lambda = \omega^i$, 对某个 i 成立. 于是 $X = X_i$.

反过来，显然 $X_i(a) = \omega^i$ 可确定 G 的一个不可约表示. □

定理 1.18 设

$$G = \langle a_1 \rangle \times \cdots \times \langle a_s \rangle$$

是有限交换群，其中 $o(a_i) = n_i$, $i = 1, \cdots, s$. 于是 $|G| = n = \prod_{i=1}^{s} n_i$. 又设域 $\mathbf{F}$ 包含 n 次本原单位根 ω, 且 $\operatorname{char} \mathbf{F} = 0$ 或 p, $(p, n) = 1$. 则 G 恰有 n 个不可约表示

$$X_{i_1 \cdots i_s}, \ i_1 = 1, \cdots, n_1; \cdots; i_s = 1, \cdots, n_s.$$

它们都是 1 级表示，且可由下式确定：

$$X_{i_1 \cdots i_s}(a_j) = \omega_j^{i_j}, \ j = 1, \cdots, s, \tag{1.2}$$

其中 ω_j 是任一 n_j 次本原单位根.

证 由定理 1.16, G 的每个不可约表示都是 1 级的. 因此它们可由基元素 $a_1, \cdots, a_s$ 对应的值唯一确定. 又由定理 1.17, a_j 只能对应到 ω_j 的方幂. 故 G 的每个不可约表示均有 (1.2) 式之形状. 反过来, (1.2) 式显然可确定 G 的一组不可约表示, 并且它们互不相同. 由此得 G 恰有 n 个由 (1.2) 式确定之不可约表示. □

在定理 1.18 中, 如果假定 $\operatorname{char} \mathbf{F} = p$ 且 $p \mid n$, G 的不可约表示也很容易确定. (注意这时要假定域 $\mathbf{F}$ 包含 m 次本原单位根, 其中 m 是 n 的 p'-部分.) 由 G 交换, $O_p(G)$ 是 G 的 Sylow p-子群. 而由命题 1.10, 对 G 的任一不可约表示 X 都有 $O_p(G) \leq \operatorname{Ker} X$. 于是 G 的不可约表示和 $\overline{G} = G/O_p(G)$ 的不可约表示是一样的. 而对后者有 $(p, |\overline{G}|) = 1$, 故可应用定理 1.18 确定之.

§2. 群代数和模

为了进一步研究群的表示, 我们需要代数和模的概念, 并且要引进代数的表示, 把群表示和代数的表示联系起来研究. 联系二者的桥梁是群代数的概念. 下面我们先来叙述这些基本概念, 其中的大部分在抽象代数课程中已经熟知.

定义 2.1 设 $\mathbf{F}$ 是域, A 是 $\mathbf{F}$ 上的有限维向量空间, 同时又是一个 (有单位元 1 的) 环. 假定对任意的 $\lambda \in \mathbf{F}$, $x, y \in A$, 恒有

$$(\lambda x)y = \lambda(xy) = x(\lambda y),$$

则称 A 为一个 $\mathbf{F}$-代数, 或简称 代数.

$\mathbf{F}$-代数最典型的例子是

例 2.2 设 $V = V(n, \mathbf{F})$ 是 $\mathbf{F}$ 上 n 维向量空间. 则 V 到自身的全体线性变换的集合 $\operatorname{End}_{\mathbf{F}}(V)$ 在通常定义的加法、乘法和数乘之下成一 $\mathbf{F}$-代数. 它的维数是 n^2, 并且与 $\mathbf{F}$ 上的全体 $n \times n$ 矩阵组成的 $\mathbf{F}$-代数 $M_n(\mathbf{F})$ 同构, 后者的运算为矩阵的加法、乘法和数乘.

和环一样，对于 **F**-代数来说也有诸如子代数，(左、右、双边) 理想，商代数，代数同态等概念，并成立同态基本定理. 我们简单叙述如下：

设 A 是 **F**-代数，B 是 A 作为向量空间的子空间，如果 B 同时也是 A 作为环的子环 (要求有 1) 或 (左、右、双边) 理想，则称 B 为 **F**-代数 A 的子代数或 (左、右、双边) 理想. 再设 B 是 A 的 (双边) 理想，则 A 作为环的商环 A/B 自然有一线性空间的结构，(或者 A 作为线性空间的商空间 A/B 自然有一环的结构)，这使 A/B 亦成一 **F**-代数，叫做 A 关于理想 B 的 **商代数**. 关于 **F**-代数的同态以及同态基本定理也和环十分相似，这里不再仔细叙述. 我们只提醒读者注意一点：因为 **F**-代数有单位元 1, 我们要求代数同态除保持运算外还把单位元映到单位元，也要求子代数包含原代数的单位元 1.

下面的群代数的概念是非常重要的.

定义 2.3 设 **F** 是域，$G=\{1=a_1,a_2,\cdots,a_g\}$ 是一个有限群，其中 $g=|G|$. 令

$$\mathbf{F}[G]=\{\sum_{i=1}^{g}\lambda_i a_i \mid \lambda_i\in\mathbf{F}\}$$

是 G 中元素用 **F** 中元素 (以下叫做数) 作系数的所有形式线性组合. 规定

$$\sum_i \lambda_i a_i=\sum_i \lambda_i' a_i \Leftrightarrow \lambda_i=\lambda_i',\ \forall i.$$

并在 **F**$[G]$ 中如下自然地规定加法和数乘

$$\sum_i \lambda_i a_i+\sum_i \lambda_i' a_i=\sum_i(\lambda_i+\lambda_i')a_i,$$

$$\lambda(\sum_i \lambda_i a_i)=\sum_i(\lambda\lambda_i)a_i,\ \forall\lambda_i,\lambda_i',\lambda\in\mathbf{F},$$

这使得 **F**$[G]$ 成为 **F** 上 g 维向量空间. 再规定乘法为

$$(\sum_i \lambda_i a_i)(\sum_j \lambda_j' a_i)=\sum_{i,j}(\lambda_i\lambda_j')(a_ia_j),$$

则易证 $\mathbf{F}[G]$ 成为一个 g 维 $\mathbf{F}$-代数，叫做群 G 在 $\mathbf{F}$ 上的**群代数**.

群代数的概念的意义在于通过它把群和代数，因而也把群的表示和代数的表示联系了起来．而代数作为环和向量空间有更丰富的结构性质，因而也更便于对它进行研究．

下面定义代数的表示.

定义 2.4 设 A 是一个 $\mathbf{F}$-代数，V 是 $\mathbf{F}$ 上的 n 维向量空间．我们称代数同态 $X : A \to \mathrm{End}_{\mathbf{F}}(V)$ 为 A 的一个**线性表示**，而称 $X : A \to M_n(\mathbf{F})$ 为 A 的一个**矩阵表示**.

和群的表示一样，我们称 V 为**表示空间**，$n = \dim_{\mathbf{F}}V$ 为**表示的级**．表示的核 $\mathrm{Ker}\, X$ 是 A 的一个 (双边) 理想．当然也有忠实表示，平凡表示，表示的等价等概念．但须注意，这里表示核 $\mathrm{Ker}\, X$ 是由 A 中映到 V 的零变换的全体所组成的，而群表示的核则由 G 中映到 V 的恒等变换的元素组成，二者从概念上是有区别的.

有了群代数的概念，我们可以把群表示和它的群代数的表示联系起来．若给了群 G 在 $\mathbf{F}$ 上的表示 X，我们把它线性扩展到 $\mathbf{F}[G]$ 上就得到 $\mathbf{F}[G]$ 的一个表示；反过来，若给了 $\mathbf{F}[G]$ 的一个表示，把它限制到 G 上，即可得到群 G 的一个表示．(注意，因为代数同态把单位元映到单位元，所以群代数 $\mathbf{F}[G]$ 中的可逆元素，特别地，G 的所有元素，必映到 $\mathrm{End}_{\mathbf{F}}(V)$ 中的可逆元素，即 V 的可逆线性变换.) 因此，研究群表示和它的群代数的表示就是一回事．我们甚至从符号上也不加区别：给了群的表示 X，它对应的群代数 $\mathbf{F}[G]$ 的表示也用符号 X.

在研究群表示时，我们引进了 G-空间的概念，并把群表示的研究化为 G-空间的研究．这里我们引进代数 A 上的模的概念，把 A 的表示和 A-模建立对应关系，以便能用模论的方法来研究表示论.

定义 2.5 设 A 是一个 $\mathbf{F}$-代数，V 是 $\mathbf{F}$ 上 n 维向量空间．假如对每个 $v \in V$, $x \in A$, 有唯一确定的元素 $vx \in V$, 并且对所有的 $x, y \in A$, $v, w \in V, \lambda \in \mathbf{F}$ 成立.

(1) $(v+w)x = vx + wx$,

(2) $v(x+y) = vx + vy$,

(3) $(vx)y = v(xy)$,

(4) $(\lambda v)x = \lambda(vx) = v(\lambda x)$,

(5) $v \cdot 1 = v$,

则称 V 为一个 (右)A-模.

容易看出, 上述条件 (1) 和 (4) 的前半表明任意的 $x \in A$ 在 V 上作用都是 V 的一个线性变换, 我们用 $X(x)$ 表示. 而条件 (2), (3) 和 (4) 的后半表明对应 $x \mapsto X(x)$ 保持加法、乘法和数乘运算, 条件 (5) 又表明这个对应 X 把 A 的单位元 1 变到 $\mathrm{End}_{\mathbf{F}}(V)$ 的单位元, 于是 X 是 A 到 $\mathrm{End}_{\mathbf{F}}(V)$ 内的代数同态. 由此看来, 一个 A-模 V 可看成是一个向量空间 V 加上一个代数同态 $X: A \to \mathrm{End}_{\mathbf{F}}(V)$, 这个同态 X 就给出了 A 的一个表示. 而且反过来, 由 A 的任一线性表示 X 出发, 规定

$$vx = v^{X(x)}, \ \forall x \in A, v \in V,$$

可使 V 成为一个 A-模. 这样, 对代数 A 的表示的研究和 A-模的研究就可以等同起来了. 这正和 G-空间与群 G 的表示可等同看待一样.

和 G-空间的情况一样, 我们可以定义 A-模的子模, 子模的和与直和, 以及 A-模的可约、不可约、可分解、不可分解等概念. 还可定义与 A-模对应的 A 的表示的上述概念. 这里不一一叙述了, 请读者自行叙述这些概念的严格定义.

又, 若取 $A = \mathbf{F}[G]$, 则 A-模和 G-空间亦可等同看待. 这正和群 G 的表示与 $\mathbf{F}[G]$ 的表示可等同看待一样. 这样我们就把 G 的表示与 $\mathbf{F}[G]$ 的表示、 $\mathbf{F}[G]$ 的表示、 G-空间、 $\mathbf{F}[G]$-模都统一起来了. 把其中之一弄清楚了, 其它的也就清楚了. 在后面的两节中, 我们将集中精力于 $\mathbf{F}[G]$-模, 研究它的构造, 并从而推出群表示的若干基本结论.

例 2.6 设 A 是一个 $\mathbf{F}$-代数. 则 A 作为 $\mathbf{F}$ 上的向量空间可以自然地看成一个 A-模, 即规定 A 的元素在 A 上的作用为右乘变

换. 这个 A-模叫做代数 A 的 (右) 正则 A-模. 我们也用符号 A 来表示.

群 G 的正则表示所对应的 $\mathbf{F}[G]$-模就是右正则 $\mathbf{F}[G]$-模. 它在群表示的研究中占据重要的地位.

还有一个重要概念是下面的

定义 2.7 设 V 是一个 A-模, 称

$$\mathrm{Ann}(V) = \{x \in A \mid vx = 0,\ \forall v \in V\}$$

为 V 的零化子.

容易验证, $\mathrm{Ann}(V)$ 是 A 的双边理想. 事实上, 如果用 X 表示对应于 A-模 V 的 A 的表示, 则 $\mathrm{Ann}(V) = \mathrm{Ker}\ X$, 且 $A/\mathrm{Ann}(V)$ 同构于 A 在 X 下的像 $X(A)$, 它是 $\mathrm{End}_{\mathbf{F}}(V)$ 的一个子代数. 并且 A-模 V 亦可看成是一个 $X(A)$-模.

还容易验证, 同构的 A-模有相同的零化子 (习题 36), 这个事实以后常常要用到.

最后提一下模同态的概念. 设 V, W 是两个 A-模. φ 是 V 到 W 作为线性空间的线性映射, 同时满足

$$(vx)^{\varphi} = (v^{\varphi})x,\ \forall v \in V, x \in A,$$

则称 φ 为 A-模 V 到 A-模 W 的一个 A-模同态. V 到 W 的所有 A-模同态的集合记作 $\mathrm{Hom}_A(V, W)$, 它是 $\mathrm{Hom}_{\mathbf{F}}(V, W)$ 的子集. 而 A-模 V 到自身的 A-同态, 即 V 的 A-模自同态的全体记作 $\mathrm{End}_A(V)$, 它是 $\mathrm{End}_{\mathbf{F}}(V)$ 的子集. 自然, 还可定义 A-模同构和 A-模自同构的概念, 请读者自行叙述.

容易验证, $\mathrm{Hom}_A(V, W)$ 在如下定义的加法和数乘之下成为 $\mathbf{F}$ 上的一个向量空间: 对于 $\varphi, \psi \in \mathrm{Hom}_A(V, W)$, $\lambda \in \mathbf{F}$, $v \in V$, 规定

$$v^{\lambda\varphi} = \lambda v^{\varphi}, v^{(\varphi+\psi)} = v^{\varphi} + v^{\psi}.$$

而 $\mathrm{End}_A(V)$ 不仅是一个 $\mathbf{F}$-向量空间, 而且若以映射的合成作为乘法还组成一个 $\mathbf{F}$-代数, 读者试证明 $\mathrm{End}_A(V)$ 恰为 $X(A)$ 在 $\mathrm{End}_{\mathbf{F}}(V)$ 中的中心化子.

§3. 不可约模和完全可约模

群表示论的基本问题之一是决定群 G 在域 $\mathbf{F}$ 上的所有不等价的不可约表示, 而这等价于决定所有互不同构的不可约 $\mathbf{F}[G]$-模. 为了解决这个问题, 我们先来研究不可约模.

定义 3.1 设 A 是 $\mathbf{F}$-代数, V 是 A-模. 称 V 为不可约的, 如果 $V \neq 0$, 且除掉 $\{0\}$ 和 V 本身外, V 没有其它的 A-子模.

不可约模的基本性质是下面的

引理 3.2 (Schur) *设 V, W 是不可约 A-模, 则 $\mathrm{Hom}_A(V,W)$ 的每个非零元素在 $\mathrm{Hom}_A(W,V)$ 中有逆.*

证 设 $\varphi \in \mathrm{Hom}_A(V,W)$, 且 $\varphi \neq 0$. 则 $\mathrm{Ker}\,\varphi$ 是 V 的子模且 $\neq V$. 而 V^φ 是 W 的子模且 $\neq 0$. 由 V 和 W 的不可约性即得到 $\mathrm{Ker}\,\varphi = 0$, $V^\varphi = W$. 于是 φ 是 V 到 W 的一一映射, 因而是 A-模同构. 于是 φ 存在逆映射 $\varphi^{-1} \in \mathrm{Hom}_A(W,V)$. □

由此立即得到

推论 3.3 *设 V 是不可约 A-模, 则 $\mathrm{End}_A(V)$ 是 $\mathbf{F}$ 上可除代数.*

定理 3.4 *设 V 同推论3.3, 又设 $\mathbf{F}$ 是代数封闭域. 则 $\mathrm{End}_A(V) \cong \mathbf{F}\cdot 1 = \{\lambda\cdot 1 \mid \lambda \in \mathbf{F}\}$, 这里 1 表 V 的恒等变换.*

证 显然 $\mathbf{F}\cdot 1 \subseteq \mathrm{End}_A(V)$. 今设 $0 \neq \varphi \in \mathrm{End}_A(V)$. 因为 φ 是有限维向量空间 V 的线性变换, 且 $\mathbf{F}$ 是代数封闭域, 则 φ 在 $\mathbf{F}$ 中有特征值 λ. 这时 $\varphi - \lambda\cdot 1$ 是降秩变换. 但由推论 3.3, $\mathrm{End}_A(V)$ 的每个非零元素都是满秩的, 故必有 $\varphi - \lambda\cdot 1 = 0$, 即 $\varphi = \lambda\cdot 1 \in \mathbf{F}\cdot 1$. □

定义 3.5 设 A 是 $\mathbf{F}$-代数, V 是 A-模. 称 V 为完全可约的, 如果对 V 的任一子模 W, 都存在另一子模 U 使 $V = W \oplus U$, 这里 "$\oplus$" 表模的直和.

注意，按照这个定义，不可约模都是完全可约模；并且容易验证完全可约模的子模也是完全可约模. (见习题 37.)

下面的定理给出了完全可约模的两个充要条件.

定理 3.6 设 V 是 A-模，则下列陈述等价：

(1) V 是完全可约模；

(2) V 是不可约模的和；

(3) V 是不可约模的直和.

证 (1) $\Rightarrow$ (2): 用对 $n = \dim_{\mathbf{F}} V$ 的归纳法. 任取 V 的一个不可约子模 $W \neq 0$, 则由完全可约性有 V 的子模 U 使 $V = W \oplus U$. 这时有 $\dim_{\mathbf{F}} U < n$. 根据归纳假设，U 可表成不可约模的直和，于是 V 有同样的表示.

(2) $\Rightarrow$ (3): 设 $V = \sum\limits_i V_i$, V_i 是不可约的 A-模. 假设 W 是 V 的能表成某些 V_i 的直和的 (在包含关系之下) 极大的子模，我们断言必有 $W = V$. 若否，必有某个 $V_j \not\subseteq W$. 则由 V_j 的不可约性有 $V_j \cap W = 0$. 于是 $V_j + W$ 仍为直和，与 W 的极大性相矛盾.

(3) $\Rightarrow$ (1) : 设 $V = \bigoplus_i V_i$ 是不可约 A-模 V_i 的直和. 又设 W 是 V 的任一子模. 取 U 为 V 的满足 $U \cap W = 0$ 的 (在包含关系之下) 极大的子模. 我们断言必有 $V = W + U$, 从而 $V = W \oplus U$. 若否，必有某个 $V_j \not\subseteq W \oplus U$, 于是由 V_j 的不可约性有 $V_j \cap (W \oplus U) = 0$, 即 $V_i + (W \oplus U) = V_j \oplus W \oplus U$ 是直和. 这时将有 $W \cap (V_j \oplus U) = 0$, 与 U 的选择相矛盾. □

对于任意的 $\mathbf{F}$-代数 A 来说，不一定每个 A-模都是完全可约的. 于是我们有

定义 3.7 称 $\mathbf{F}$-代数 A 为**半单代数**, 如果任一 A-模 V 都是完全可约的.

定理 3.8 设 A 为 $\mathbf{F}$-代数. 如果右正则模 A 是完全可约的，则 A 为半单代数.

证　由定义 3.7, 只需证任一 A-模 V 都是完全可约的. 又因为任一 A-模 V 都可表成若干个循环模 (即由一个元素生成的模) 的和, 根据定理 3.6(2), 又只需对 $V = vA$ 是循环模的情形来证明. 考虑映射 $\varphi : a \mapsto va$, $\forall a \in A$. 显然 φ 是正则模 A 到 V 的同态. 于是由同态基本定理有 $V \cong A/\mathrm{Ker}\ \varphi$, 这里 $\mathrm{Ker}\ \varphi$ 是正则模 A 的子模. 根据 A 的完全可约性, 有 A 的子模 U 使得 $A = \mathrm{Ker}\ \varphi \oplus U$. 于是有 $V \cong U$. 因为 U 作为完全可约模 A 的子模仍为完全可约的 (习题 37), 故 V 亦完全可约. □

下面的定理对于整个表示论来说是极其重要的.

定理 3.9 (Maschke) *设 G 是有限群, $\mathbf{F}$ 是域. 若 $\mathrm{char}\ \mathbf{F} = 0$ 或 $\mathrm{char}\ \mathbf{F} = p$, 但 $p \nmid |G|$, 则群代数 $\mathbf{F}[G]$ 是半单的.*

证　设 V 是任一 $\mathbf{F}[G]$-模, W 是它的子模. 首先, 我们可以找到 V 的子空间 U 使得 $V = W \oplus U$, 但这里 U 不一定是 $\mathbf{F}[G]$-子模. 考虑由这个分解得到的 V 到 W 上的射影 φ, 这时 φ 是 $\mathbf{F}$-同态但不一定是 $\mathbf{F}[G]$-同态. 现在如下规定 V 到 W 上的另一映射 ψ:

$$v^{\psi} = |G|^{-1} \sum_{a \in G} (va)^{\varphi} a^{-1},$$

其中 $|G|^{-1}$ 表 $\mathbf{F}$ 中元素 $|G|$ 的逆, 因为 $\mathrm{char}\ \mathbf{F} = 0$ 或 p, $p \nmid |G|$, 则 $|G|^{-1}$ 总是存在的. 我们要证明 ψ 是 V 到 W 上的 $\mathbf{F}[G]$-同态.

首先, 显然有 ψ 是 V 到 W 的 $\mathbf{F}$-同态. 又, 对于任意的 $x \in G$, 有

$$\begin{aligned}(vx)^{\psi} &= |G|^{-1} \sum_{a \in G} (vxa)^{\varphi} a^{-1} \\ &= |G|^{-1} \sum_{a \in G} (v(xa))^{\varphi} (xa)^{-1} x \\ &= v^{\psi} x.\end{aligned}$$

这证明了 ψ 是 $\mathbf{F}[G]$-同态.

如果 $v \in W$. 由 $va \in W$, $\forall a \in G$, 有 $(va)^{\varphi} = va$, 于是

$$\begin{aligned} v^{\psi} &= |G|^{-1}\sum_{a\in G}(va)^{\varphi}a^{-1} \\ &= |G|^{-1}\sum_{a\in G}vaa^{-1} \\ &= |G|^{-1}\sum_{a\in G}v = |G|^{-1}|G|v = v. \end{aligned}$$

这说明 ψ 是 V 到 W 上的 $\mathbf{F}[G]$-同态. 令 $\operatorname{Ker}\psi = K$. 显然 K 也是 $\mathbf{F}[G]$-模. 我们要证明 $V = W \oplus K$. 首先, 对任意的 $v \in V$, 有 $v^{\psi} \in W$. 而因

$$(v - v^{\psi})^{\psi} = v^{\psi} - (v^{\psi})^{\psi} = v^{\psi} - v^{\psi} = 0,$$

知 $v - v^{\psi} \in K$. 于是 $v = v^{\psi} + (v - v^{\psi}) \in W + K$. 这说明 $V = W + K$. 再设 $k \in K \cap W$. 由 $k \in W$, 有 $k^{\psi} = k$; 而由 $k \in K$ 有 $k^{\psi} = 0$, 于是 $k = 0$, 这说明 $K \cap W = 0$. 这样我们证明了 $V = W \oplus K$. □

Maschke 定理的逆也成立, 即我们有

定理 3.10 *设 G 是有限群, $\mathbf{F}$ 是域. 如果 $\mathbf{F}[G]$ 是半单的, 则若 $\operatorname{char}\mathbf{F} \neq 0$, 必有 $\operatorname{char}\mathbf{F} \nmid |G|$.*

证 用反证法, 设 $\operatorname{char}\mathbf{F} \mid |G|$. 考虑正则模 $\mathbf{F}[G]$ 的一维子模 $\langle c\rangle$, 其中 $c = \sum_{a\in G} a$. 由 $\mathbf{F}[G]$ 的半单性, $\mathbf{F}[G]$ 有 $g-1$ 维子模 W 使 $\mathbf{F}[G] = \langle c\rangle \oplus W$. 因为

$$c^2 = (\sum_{a\in G} a)^2 = |G|\sum_{a\in G} a = |G|c = 0,$$

故 $c = 1\cdot c \in \mathbf{F}[G]\cdot c \subseteq W$, 与 $\langle c\rangle \cap W = 0$ 相矛盾. □

Maschke 定理的意义在于揭示了有限群的表示和基域的特征之间的关系. 如果 $\operatorname{char}\mathbf{F} = 0$ 或 $\operatorname{char}\mathbf{F} = p$ 但 $p \nmid |G|$, 则群 G 在域 $\mathbf{F}$ 上的每个表示都是完全可约的. 因此对群 G 的任意表示的

研究就可化归为对于不可约表示的研究. 换句话说, 不可约表示研究清楚了, 群的所有表示也就清楚了. 但如果 char $\mathbf{F} \mid |G|$, 情况就大不相同了. 它比前种情况要复杂的多. 我们称前种情况为有限群的常表示, 而称 char $\mathbf{F} \mid |G|$ 的情况为模表示. 在本章的以下部分, 我们只来研究有限群的常表示.

§4. 半单代数的构造

前面说过, 由于有了 Maschke 定理, 研究有限群的常表示只需研究它的不可约表示. 而这又等价于研究不可约 $\mathbf{F}[G]$-模. 本节的目的即通过分析半单代数的构造来找出所有互不同构的不可约 $\mathbf{F}[G]$-模.

引理 4.1 设 A 是 $\mathbf{F}$-代数, V 是不可约 A-模, 则 V 同构于正则模 A 的一个商模. 而如果 A 是半单代数, 则 V 同构于正则模 A 的一个不可约子模.

证 任取 $0 \neq v \in V$, 则循环模 vA 是 V 的非零子模. 由 V 的不可约性有 $vA = V$. 考虑映射 $\varphi : a \to va$, $\forall a \in A$, 易验证 φ 是正则模 A 到 V 上的 A-模同态, 于是有 $V \cong A/\mathrm{Ker}\ \varphi$, 这证明了引理的前半.

再设 A 是半单代数, 则正则模 A 是完全可约的. 于是存在 A 的子模 U 使 $A = \mathrm{Ker}\ \varphi \oplus U$, 这推出 $V \cong U$. 再由 V 的不可约性得 U 的不可约性. 这证明了引理的后半. □

这个引理告诉我们, 对于半单代数 A, 所有的不可约 A-模都同构于正则模 A 的子模, 因此, 为了找出所有互不同构的不可约 A-模, 只需在正则模 A 中去找.

根据第 III 章学过的 Krull-Schmidt 定理, 正则模 A 作为具有两个链条件的算子群, 它的分成不可分解子模 (因 A 半单, 即不可约子模) 的直和分解式从本质上来说是唯一的. 也就是说, 若不计同构以及直和因子的次序是唯一确定的. 设下面的 (4.1) 式

是这样一种分解：

$$A = M_{11}\oplus\cdots\oplus M_{1k_1}\oplus M_{22}\oplus\cdots\oplus M_{2K_2}\oplus\cdots\oplus M_{s1}\oplus\cdots\oplus M_{sk_s}, \quad (4.1)$$

其中 $M_{ij} \cong M_{i1} = M_i$, $j = 1,\cdots,k_i, i = 1,\cdots,s$, 并且 $M_1,\cdots,M_s$ 彼此互不同构. 命

$$M_i(A) = M_{i1} \oplus \cdots \oplus M_{ik_i},\ i = 1,\cdots,s, \quad (4.2)$$

于是又有

$$A = M_1(A) \oplus M_2(A) \oplus \cdots \oplus M_s(A). \quad (4.3)$$

由 Krull-Schmidt 定理，在上面诸分解式中出现的数 s 和 $k_1,\cdots,k_s$ 都是唯一确定的. 并且，只可能有 s 个 (有限多个) 互不同构的不可约 A-模，$M_1,\cdots,M_s$ 就是一组完全代表系. 更进一步，我们还有：

引理 4.2 对于 $i = 1,\cdots,s$,

(1) (4.3) 式中的 $M_i(A)$ 恰为 A 中所有与 M_i 同构的子模之和，因而被 A 所唯一确定；

(2) 对于 $i \neq j$, $M_i(A) \cap M_j(A) = 0$;

(3) $M_i(A)$ 不仅是 A-模，而且还可看成是 E-模，这里 $E = \mathrm{End}_A(A)$.

证 (1) 若有 A 的子模 $M \cong M_i$, 但 $M \not\subseteq M_i(A)$, 则 $M + M_i(A) = M \oplus M_i(A)$. 由 A 的完全可约性，有 A 的子模 U 使 $A = M \oplus M_i(A) \oplus U$. 把它们都分解为不可约子模的直和，则得到一个含有至少 $k_i + 1$ 个同构于 M_i 的不可约子模的直和分解式，与 Krull-Schmidt 定理相矛盾. 这样 $M \subseteq M_i(A)$, 即 $M_i(A)$ 是 A 中所有同构于 M_i 的子模直和.

(2) 设 $i \neq j$, 且 $M_i(A) \cap M_j(A) \neq 0$, 取 A 的一个不可约子模 $W \subseteq M_i(A) \cap M_j(A)$. 因为 $W \subseteq M_i(A)$, 必有 $W \cong M_i$. (若否，由 $M_i(A)$ 的完全可约性可得 $M_i(A)$ 的一个直和分解式以 W 为某一项，但 $M_i(A)$ 又有分解式 (4.2), 将与 Krull-Schmidt 定理相违背.

(3) 对任意的 $\varphi \in E = \mathrm{End}_A(A)$, 我们证明 $M_i(A)^\varphi \subseteq M_i(A)$. 由 (1), $M_i(A)$ 为 A 中同构于 M_i 的子模之和. 设 M 是一个这样的子模, 我们只需证明 $M^\varphi \subseteq M_i(A)$. 若 $M^\varphi = 0$, 当然有上述结论; 而若 $M^\varphi \neq 0$, 由 Schur 引理, 必有 $M^\varphi = M_i$, 于是也有 $M^\varphi \subseteq M_i(A)$, 得证. □

定理 4.3 (**Wedderburn**) 设 A 是域 $\mathbf{F}$ 上半单代数, 则

(1) (4.3) 式中每个 $M_i(A)$ 是 A 作为代数的双边理想;

(2) 对于任意不可约 A-模 W, 如果 $W \cong M_i$, 则

$$\mathrm{Ann}(W) = M_1(A) \oplus \cdots \oplus M_{i-1}(A) \oplus M_{i+1}(A) \oplus \cdots \oplus M_s(A). \quad (4.4)$$

又设 X_i 是由 W 得到的 A 的表示, 则 $X_i(A) \cong M_i(A)$;

(3) 每个 $M_i(A)$ 是 A 的极小 (双边) 理想, 因此, $M_i(A)$ 是 $\mathbf{F}$ 上的单代数, 即没有非平凡双边理想的代数. 这样, 域 $\mathbf{F}$ 上任一半单代数都可分解为单代数的直和.

证 (1) 正则模 A 的每个子模都是 A(作为代数) 的右理想, 因此 $M_i(A)$ 是 A 的右理想. 又对于任一 $x \in A$, A 的左乘变换 $\varphi_x : a \mapsto xa$, $a \in A$, 显然是正则模 A 的一个 A-同态, 即 $\varphi_x \in E = \mathrm{End}_A(A)$. 根据引理 4.2(3), $M_i(A)$ 也是 E-模, 于是 $M_i(A)\varphi_x \subseteq M_i(A)$. 这说明 $xM_i(A) \subseteq M_i(A)$, 即 $M_i(A)$ 也是 A 的左理想.

(2) 因为同构的 A-模有相同的零化子, 故可设 $W = M_i \subseteq M_i(A)$. 由 (1), $M_i(A)$ 是 A 的双边理想, 故对 $i \neq j$, 有

$$M_i(A)M_j(A) \subseteq M_i(A) \cap M_j(A) = 0.$$

于是

$$\mathrm{Ann}(W) \supseteq M_1(A) \oplus \cdots \oplus M_{i-1}(A) \oplus M_{i+1}(A) \oplus \cdots \oplus M_s(A).$$

又, 设 $0 \neq x \in M_i(A)$, 我们证明 $x \notin \mathrm{Ann}(W)$. 若否, 则由 $Wx = 0$ 推知对任一 $j = 1, \cdots, k_j$, 有 $M_{ij}x = 0$, 于是有 $M_i(A)x = 0$. 又, 刚才已证对 $j \neq i$ 有 $M_i(A)x = 0$, 于是据 (4.3) 式有 $Ax = 0$. 但 $x = 1 \cdot x \in Ax = 0$, 这样得到 $x = 0$, 矛盾.

至此我们即可断言 (4.4) 式成立. 若否, 有

$$x \notin M_1(A) \oplus \cdots \oplus M_{i-1} \oplus M_{i+1} \oplus \cdots \oplus M_s(A).$$

但 $x \in \mathrm{Ann}(W)$, 则 x 的第 i 个分量 $x_i \neq 1$ 且 $x_i \in \mathrm{Ann}(W)$, 矛盾.

最后, 由 (4.4) 式即可得到

$$X_i(A) = A/\mathrm{Ann}(W) \cong M_i(A).$$

(3) 假定 $M_i(A)$ 非单, 即它有非平凡双边理想 I. 则由 (4.3) 式, I 也是 A 的双边理想. 取 $M_i(A)$ 的一个不可约 A-子模 $W \not\subseteq I$, 则由 W 的不可约性有 $W \cap I = 0$. 再由 I 是双边理想, 有 $WI \subseteq W \cap I = 0$, 于是 $I \subseteq \mathrm{Ann}(W)$, 与 (2) 矛盾. □

为了进一步弄清半单代数 A 的结构, 还要研究单代数 $M_i(A)$ 的构造. 由上面的定理 4.3 知, $M_i(A) \cong X_i(A)$, 这里 X_i 是由不可约 A-模 M_i 得到的 A 的表示. 因此我们只需研究 $X_i(A)$ 的构造. 我们有下面的

定理 4.4 (双中心化子定理) *设 A 是半单 F-代数, M_i 是不可约 A-模, 令 $E_i = \mathrm{End}_A(M_i)$, 则 M_i 亦可看成 E_i-模, 并且有 $\mathrm{End}_{E_i}(M_i) = X_i(A)$.*

证 首先注意, 定理中并未假定 $M_i \subseteq A$. 但因把 M_i 换成与它同构的 A-模后并不影响结论的正确性, 因而不失普遍性可设 $M_i \subseteq A$, 并且就是前面规定的 M_i, 这时有 $M_i \subseteq M_i(A)$, 且 $M_i(A) \cong X_i(A)$.

把 M_i 看成 E_i-模, 由 $E_i = \mathrm{End}_A(M_i)$ 的定义有 $X_i(A) \subseteq \mathrm{End}_{E_i}(M_i)$. 为证相反方向的包含关系, 我们设 $\theta \in \mathrm{End}_{E_i}(M_i)$, 于是有

$$(v^\alpha)^\theta = (v^\theta)^\alpha, \ \forall \alpha \in E_i, v \in M_i.$$

给定一个 $v \in M_i$, 考虑 M_i 到 A 的映射 $\alpha_v : m \mapsto vm, m \in M_i$. 因为 M_i 是 A 的右理想, 有 $vm \in M_i$, 故 α_v 是 M_i 到 M_i 的映射.

明显地，α_v 是 M_i 的线性映射，即 $\alpha_v \in \mathrm{End}_{\mathbf{F}}(M_i)$. 又因为对任意的 $a \in A$，有

$$(ma)^{\alpha_v} = v(ma) = (vm)a = (m^{\alpha_v})a,$$

故 α_v 是 M_i 的 A-模自同态，即 $\alpha_v \in \mathrm{End}_A(M_i) = E_i$. 于是对任意的 $v, w \in M_i$，有

$$(vw)^\theta = (w^{\alpha_v})^\theta = (w^\theta)^{\alpha_v} = v(w^\theta) \tag{4.5}$$

现在固定一个 $w \in M_i$, $w \neq 0$, 有 $AwA \subseteq M_i(A)$, 又因 AwA 是 A 的双边理想，且 $0 \neq w = 1 \cdot w \cdot 1 \in AwA$, 故 $AwA \neq 0$. 由 $M_i(A)$ 的极小性有 $AwA = M_i(A)$. 再设 e 是单代数 $M_i(A)$ 的单位元，有 $e \in AwA$, 于是 $e = \sum\limits_j a_j w b_j$, 其中 $a_j, b_j \in A$. 这时我们有

$$v = ve = v\sum_j a_j w b_j = \sum (va_j)(wb_j),$$

其中 $va^j, wb_j \in M_i$, 在等式 (4.5) 中以 va_j 代替 v, wb_j 代替 w, 得到

$$((va_j)(wb_j))^\theta = va_j(wb_j)^\theta.$$

于是有

$$v^\theta = (\sum_j (va_j)(wb_j))^\theta = \sum_j (va_j)(wb_j)^\theta = v\sum_j a_j(wb_j)^\theta,$$

这样 $\theta = X_i(\sum\limits_j a_j(wb_j)^\theta)$, 即 $\theta \in X_i(A)$. □

根据 Schur 引理，上述定理中的 E_i 是 $\mathbf{F}$ 上的可除代数. 而若 $\mathbf{F}$ 若是代数封闭域，则更有 $E_i \cong \mathbf{F} \cdot 1$. 于是我们有

推论 4.5 设 $\mathbf{F}$ 是代数封闭域，A 是 $\mathbf{F}$ 上的半单代数，则
(1) (4.3) 式中的 $M_i(A) \cong \mathrm{End}_{\mathbf{F}}(M_i) = X_i(A)$;
(2) $\dim_{\mathbf{F}}(M_i(A)) = (\dim_{\mathbf{F}} M_i)^2$;
(3) (4.1) 式中的 $k_i = \dim_{\mathbf{F}} M_i$;

(4) $\dim_{\mathbf{F}} A = \sum_{i=1}^{s} (\dim_{\mathbf{F}} M_i)^2$;

(5) 设 A 的中心为 $Z(A)$, 则 $s = \dim_{\mathbf{F}} Z(A)$.

证 由定理 3.4, $\mathrm{End}_A(M_i) \cong \mathbf{F} \cdot 1$, 再由定理 4.4, 即得 (1). 又由 $\dim_{\mathbf{F}}(\mathrm{End}_{\mathbf{F}}(M_i)) = (\dim_{\mathbf{F}} M_i)^2$, 即得 (2) 和 (3). 而由分解式 (4.3) 得到 (4).

为证明 (5), 设 $M_i(A)$ 的中心为 $Z(M_i(A))$. 显然, $Z(M_i(A)) \subseteq Z(A)$, 于是有

$$Z(M_1(A)) \oplus \cdots \oplus Z(M_s(A)) \subseteq Z(A).$$

又对任一 $z \in Z(A)$, 设 $z = z_1 + \cdots + z_s$, 其中 $z_i \in M_i(A)$. 则易验证 $z_i \in Z(M_i(A))$. 于是有

$$Z(M_1(A)) \oplus \cdots \oplus Z(M_s(A)) = Z(A).$$

最后, 因为 $M_i(A) \cong \mathrm{End}_{\mathbf{F}}(M_i)$, 而后者的中心仅由数乘变换组成, 故 $\dim_{\mathbf{F}}(Z(M_i(A)) = 1$. 这就推出 $\dim_{\mathbf{F}}(Z(A)) = s$. □

应用到群的表示, 我们有

定理 4.6 *设 G 是有限群, $|G| = g$, $\mathbf{F}$ 是代数封闭域, 且 $\mathrm{char}\, \mathbf{F} = 0$ 或 $\mathrm{char}\, \mathbf{F} = p$ 但 $p \nmid |G|$. 又设 G 的共轭类数为 s, 则 G 恰有 s 个不等价的不可约表示 $X_1 = 1_G, X_2, \cdots, X_s$. 假定 X_i 的级 $\deg X_i = n_i$, 则 $g = \sum_{i=1}^{s} n_i^2$.*

证 由定理的条件, $\mathbf{F}[G]$ 为 $\mathbf{F}$ 上的半单代数. 根据推论 4.5, 只需证明 $\dim_{\mathbf{F}}(Z(\mathbf{F}[G]))$ 等于 G 的共轭类数 s 就可得到定理的全部结论. 首先, 对于 G 的任一共轭类 C_i, 令 $c_i = \sum_{a \in C_i} a$, 则 $c_i \in Z(\mathbf{F}[G])$. (这因为对任一 $x \in G$, 有 $x^{-1} c_i x = \sum_{a \in C_i} x^{-1} a x = \sum_{a \in C_i} a = c_i$.) 因为 $c_1, \cdots, c_s$ 在 $\mathbf{F}[G]$ 中线性无关, 故 $\dim_{\mathbf{F}}(Z(\mathbf{F}[G])) \geq s$. 另一方面, 设 $z \in Z(\mathbf{F}[G])$, 并令 $z = \sum_{i=1}^{g} \lambda_i a_i$, $\lambda_i \in \mathbf{F}$. 则对任一

$x \in G$, 有 $x^{-1}zx = z$, 即

$$\sum_{i=1}^{g} \lambda_i a_i = \sum_{i=1}^{g} \lambda_i x^{-1} a_i x.$$

这说明属于同一共轭类的元素 a_i 前面的系数 λ_i 必相等. 于是 z 可表成诸 c_i 的线性组合, 因此诸 c_i 组成 $Z(\mathbf{F}[G])$ 的一组基. 于是 $\dim(Z(\mathbf{F}[G])) = s$. □

§5. 特征标, 类函数, 正交关系

从本节起, 为了使叙述方便, 我们更假定基域 $\mathbf{F}$ 是复数域 $\mathbb{C}$, 因为 $\mathbb{C}$ 是特征 0 的代数闭域, 每个 $\mathbb{C}$ 上的表示都是完全可约的, 并且上节的定理 4.6 也当然成立.

研究表示的好处在于线性变换或矩阵更便于计算. 但由于 n 级矩阵包含 n^2 个数, 这又使得群表示具有过多的 "数字信息". 为了避免这种复杂性, 我们引进群特征标的概念.

定义 5.1 设 $\mathbf{X}: G \to GL(n, \mathbb{C})$ 是 G 的一个矩阵表示, 则以

$$\chi(a) = \mathrm{tr}\, \mathbf{X}(a), \ \forall a \in G,$$

定义的映射 $\chi: G \to \mathbb{C}$ 称为对应于表示 $\mathbf{X}$ 的特征标.

因为相似矩阵的迹相同, 故等价的矩阵表示具有相同的特征标. 同时这也使我们能够定义线性表示 $X: G \to GL(V)$ 的特征标. 这只须在 V 中任取一组基, 得到与 X 对应的矩阵表示 $\mathbf{X}$, 再来计算 $\mathbf{X}$ 的特征标即可. 这样计算出来的特征标与基的选取无关. 并且等价的线性表示的特征标也相同.

和表示一样, 我们称定义 5.1 中的数 n 为特征标 χ 的级. 并依所对应的表示 $\mathbf{X}$(或 X) 为忠实的, 平凡的, 可约的, 不可约的等等, 而称特征标 χ 为忠实的, 平凡的, 可约的, 不可约的. 还规定特征标 χ 的核 $\mathrm{Ker}\, \chi = \mathrm{Ker}\, \mathbf{X} = \mathrm{Ker}\, X$.

称 G 的 1 级特征标，即 1 级表示的特征标为 *线性特征标*. 特别地，称 G 的 1-表示的特征标为 *1-特征标* 或 *主特征标*, 也记作 1_G(显然 $1_G(a)=1$, $\forall a\in G$).

根据定理 1.18, 交换群的不可约特征标皆为线性特征标. 更一般地我们有

定理 5.2 *有限群 G 线性特征标的个数等于 $|G:G'|$.*

证 设 χ 是 G 的任一线性特征标，则 χ 也是 G 到 $(\mathbb{C}^{\#},\cdot)$ 内的同态. 因 $(\mathbb{C}^{\#},\cdot)$ 是交换群，故 $G'\le \mathrm{Ker}\,\chi$. 这说明 χ 也可看作是 G/G' 的线性特征标. 反之，由 G/G' 的一个线性特征标自然也可规定一个 G 的线性特征标. 因为 G/G' 是交换群，由定理 1.13, G/G' 恰有 $|G/G'|$ 个线性特征标，故 G 亦有同样多的线性特征标. □

由 G 的置换表示和正则表示得到的特征标也很常用.

例 5.3 在例 1.7 中给出的群 G 的置换表示 $\mathbf{P}$ 的特征标记作 ρ. 明显地，对于任意的 $a\in G$, $\mathbf{P}(a)$ 的主对角线上第 i 个元素为 1 的充要条件为 $i^a=i$, 即 i 为 a 的不动点. 因此我们有

$$\rho(a)=|\mathrm{fix}_{\,\Omega}(a)|,$$

其中 $\mathrm{fix}_{\,\Omega}(a)$ 表 a 在 Ω 上的不动点集合. 特别地，$\rho(1)=|\Omega|=n$.

例 5.4 例 1.8 中给出的群 G 的右正则表示 $\mathbf{R}$ 的特征标记作 r_G. 易看出对任意的 $a\in G$, 我们有

$$r_G(a)=\begin{cases}|G|, & \text{如果 } a=1,\\ 0, & \text{如果 } a\neq 1.\end{cases}$$

正则特征标 r_G 在群特征标理论中起着重要的作用.

下面的定理给出特征标的简单性质.

定理 5.5 *设 X,Y 是 G 的两个表示，χ,ψ 分别是 X,Y 的特征标，则*

(1) 若 X, Y 等价，则 $\chi = \psi$;

(2) 若 a 和 a' 在 G 中共轭，则 $\chi(a) = \chi(a')$, 从而特征标 χ 可看成是定义在 G 的共轭类上的函数;

(3) X 和 Y 的直和的特征标为 $\chi + \psi$; (这里规定 $(\chi + \psi)(a) = \chi(a) + \psi(a)$, $\forall a \in G$.)

(4) 令 $\overline{\chi}(a) = \overline{\chi(a)}$, $\forall a \in G$, 此处 $\overline{\chi(a)}$ 表 $\chi(a)$ 的复共轭，则 $\overline{\chi}$ 亦为 G 的特征标;

(5) 设 $\mathbf{X}$ 是 G 的任一矩阵表示， $a \in G$. 则 $\mathbf{X}(a)$ 相似于对角矩阵，并由此推出 $\chi(a)$ 是若干个 $o(a)$ 次单位根的和;

(6) $\chi(a^{-1}) = \overline{\chi(a)}$, $\forall a \in G$;

(7) $\chi(a)$ 的模 $|\chi(a)| = \chi(1)$ 当且仅当 $\mathbf{X}(a)$ 为纯量矩阵 (或 $X(a)$ 为数乘变换); 而 $\chi(a) = \chi(1)$ 当且仅当 $\mathbf{X}(a) = \mathbf{I}$(或 $X(a) = 1$), 其中 $\mathbf{I}$表单位矩阵， 1 表单位变换.

证 (1), (2) 由相似矩阵的迹相等立得.

(3) 显然.

(4) 设 $\mathbf{X} : G \to GL(n, \mathbb{C})$ 是具有特征标 χ 的矩阵表示，则易验证映射 $a \mapsto \overline{\mathbf{X}(a)}$, $a \in G$, 仍为 G 的矩阵表示，它所对应的指标为 $\overline{\chi}$. 上式中 $\overline{\mathbf{X}(a)}$ 表示矩阵 $\mathbf{X}(a)$ 的复共轭.

(5) 设 $o(a) = m$, 则有 $\mathbf{X}(a)^m = \mathbf{I}$, 即 $\mathbf{X}(a)$ 的极小多项式整除 $x^m - 1$, 因此无重根. 由线性代数知 $\mathbf{X}(a)$ 可用相似变换化为对角矩阵

$$\operatorname{diag}(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n) = \begin{pmatrix} \varepsilon_1 & & & 0 \\ & \varepsilon_2 & & \\ & & \ddots & \\ 0 & & & \varepsilon_n \end{pmatrix}.$$

由于 $\mathbf{X}(a)^m = \mathbf{I}$, 有 $\varepsilon_i^m = 1$, $i = 1, \cdots, n$, 即 ε_i 是 m 次单位根. 因此， $\chi(a) = \sum_{i=1}^n \varepsilon_i$ 是 n 个 m 次单位根的和.

(6) 由 (5), $\mathbf{X}(a)$ 相似于 $\operatorname{diag}(\varepsilon_1, \cdots, \varepsilon_n)$, 故 $\mathbf{X}(a^{-1})$ 相似于 $\operatorname{diag}(\varepsilon_1^{-1}, \cdots, \varepsilon_n^{-1})$. 因为 ε_i 是单位根，有 $\varepsilon_i^{-1} = \overline{\varepsilon}_i$. 故

$$\chi(a^{-1}) = \sum_{i=1}^n \varepsilon_i^{-1} = \sum_{i=1}^n \overline{\varepsilon_i} = \overline{\chi(a)}.$$

(7) 由 (6), 可设 $\chi(a) = \sum_{i=1}^{n} \varepsilon_i$, 其中 ε_i 是单位根. 又由复数加法的三角不等式，有

$$|\chi(a)| = |\sum_i \varepsilon_i| \leq \sum_i |\varepsilon_i| = n = \chi(1),$$

且等号成立仅当诸 ε_i 的幅角相等. 因此，若 $|\chi(a)| = \chi(1)$, 则诸 ε_i 相等，譬如设其值为 ε. 于是 $\mathbf{X}(a)$ 相似于纯量阵 $\varepsilon\mathbf{I}$, 当然也有 $\mathbf{X}(a) = \varepsilon\mathbf{I}$. 而若 $\chi(a) = \chi(1)$, 则可推出诸 $\varepsilon_i = 1$, 于是 $\mathbf{X}(a) = \mathbf{I}$. 反之，由 $\mathbf{X}(a)$ 是纯量阵 (或单位阵) 推出 $|\chi(a)| = \chi(1)$(或 $\chi(a) = \chi(1)$) 是明显的. □

为了研究群特征标的进一步性质，我们先来研究不可约特征标之间的关系. 事实上，由 Maschke 定理，群 G 的任一表示是不可约表示的直和；又据定理 5.5(3), 群 G 的任一特征标亦为不可约特征标的和. 因此，只要把群 G 的不可约特征标搞清楚了，群 G 的所有特征标也就清楚了.

首先我们注意到，根据定理 5.5(2), 群 G 的每个特征标都是群的所谓类函数，见下述定义.

定义 5.6 称映射 $\theta : G \to \mathbb{C}$ 为群 G 上的一个 *类函数*, 如果

$$\theta(b^{-1}ab) = \theta(a), \ \forall a, b \in G.$$

G 上所有类函数的集合记作 $Cf(G)$.

定理 5.7 *在 $Cf(G)$ 中如下规定类函数的加法和数乘，可使 $Cf(G)$ 成一 $\mathbb{C}$-空间，其维数等于 G 的共轭类数 s.*

(1) *加法*：对于 $\theta, \varphi \in Cf(G)$, 令

$$(\theta + \varphi)(a) = \theta(a) + \varphi(a), \ \forall a \in G;$$

(2) *数乘*：对于 $\theta \in Cf(G)$, $\lambda \in \mathbb{C}$, 令

$$(\lambda\theta)(a) = \lambda\theta(a), \ \forall a \in G;$$

证　可直接验证. □

根据定理 4.6, G 在 $\mathbb{C}$ 上恰有 s 个不等价的不可约表示 $X_1, \cdots, X_s$, 设它们对应的特征标为 $\chi_1, \cdots, \chi_s$. 我们要证明, 它们组成 $Cf(G)$ 的一组基, 特别地, 这些 χ_i 互不相同, 因而 G 也恰有 s 个不同的不可约特征标. 并用 $\mathrm{Irr}(G)$ 记它们组成的集合, 即 $\mathrm{Irr}(G) = \{\chi_1, \cdots, \chi_s\}$.

根据上节 (4.3) 式, 群代数 $\mathbb{C}[G]$ 有分解式

$$\mathbb{C}[G] = M_1(\mathbb{C}[G]) \oplus \cdots \oplus M_s(\mathbb{C}[G]). \tag{5.1}$$

令 $1 = \sum_{i=1}^{s} e_i$, 其中 $e_i \in M_i(\mathbb{C}[G])$. 则 e_i 是单代数 $M_i(\mathbb{C}[G])$ 的单位元. 考虑由 $\mathbb{C}[G]$-模 M_i 得到的 $\mathbb{C}[G]$ 的表示 X_i, 有

$$X_i(e_j) = \begin{cases} 0, & j \neq i, \\ 1, & j = i, \end{cases}$$

这里 0, 1 分别代表 M_i 的零变换和恒等变换, 于是特征标 χ_i (若把定义域扩展到整个 $\mathbb{C}[G]$ 上) 在 e_j 上取值为

$$X_i(e_j) = \begin{cases} 0, & j \neq i, \\ \chi_i(1), & j = i. \end{cases} \tag{5.2}$$

由 (5.2) 式易看出 $\chi_i, i = 1, \cdots, s$, 作为 $\mathbb{C}[G]$ 上的函数是线性无关的, 当然作为 G 上的函数也线性无关. 于是得到

定理 5.8 *设群 G 有 s 个共轭元素类, 则 G 在复数域 $\mathbb{C}$ 上恰有 s 个不可约特征标 $\chi_1, \cdots, \chi_s$. 它们构成 $Cf(G)$ 的一组基, 并且有*

$$\sum_{i=1}^{s} \chi_i(1)^2 = g = |G| \tag{5.3}$$

证　定理中除 (5.3) 式外的其余结论前面都已证明, 而 (5.3) 式由定理 4.6 立得. □

命题 5.9 设 $\varphi \in Cf(G)$，且 $\varphi = \sum_{i=1}^{s} \lambda_i \chi_i$，$\lambda_i \in \mathbb{C}$，则 φ 是特征标 $\Longleftrightarrow$ 每个 λ_i 都是非负整数.

证 $\Longrightarrow$：设 X 是特征标 φ 对应的表示，由完全可约性，X 可分解为不可约表示 X_i 的直和，于是特征标 φ 的分解式中诸 λ_i 皆为非负整数.

$\Longleftarrow$：设 X_i 是有特征标 χ_i 的表示．若令

$$X = \bigoplus_{i=1}^{s} \lambda_i X_i,$$

则 X 的特征标为 φ，这说明 φ 是特征标. □

定理 5.10 设 X, Y 是 G 在 $\mathbb{C}$ 上的二表示，对应的特征标为 χ 和 ψ．则 X 与 Y 等价 $\Longleftrightarrow \chi = \psi$.

证 $\Longrightarrow$：显然.

$\Longleftarrow$：把 X, Y 分解为不可约表示的直和，设

$$X \sim \bigoplus_{i=1}^{s} n_i X_i,\ Y \sim \bigoplus_{i=1}^{s} m_i X_i,$$

其中 n_i, m_i 是非负整数，符号"$\sim$"表等价．于是 X, Y 对应的特征标 χ, ψ 应满足

$$\chi = \sum_{i=1}^{s} n_i \chi_i,\ \psi = \sum_{i=1}^{s} m_i \chi_i.$$

由条件 $\chi = \psi$ 及 $\{\chi_i\}$ 为 $Cf(G)$ 的基，即推得 $n_i = m_i$，$\forall i$．故 $X \sim Y$. □

有限群的诸不可约特征标间最重要的关系是所谓的正交关系．它的证明关键是计算在 $\mathbb{C}[G]$ 中元素 e_i 的表达式．为了得到这个表达式，我们先来看看正则特征标 r_G 的两个表达式，其一已由例 5.4 中给出，其二是下面的

引理 5.11 $r_G = \sum_{i=1}^{s} \chi_i(1)\chi_i$.

证 根据定理 4.4 和推论 4.5, 正则模 $\mathbb{C}[G]$ 有分解

$$\mathbb{C}[G] = \underbrace{M_1 \oplus \cdots \oplus M_1}_{\dim_{\mathbb{C}} M_1\ 个} \oplus \cdots \oplus \underbrace{M_s \oplus \cdots \oplus M_s}_{\dim_{\mathbb{C}} M_s\ 个}.$$

故正则表示 R 也有分解

$$R = \underbrace{X_1 \oplus \cdots \oplus X_1}_{\dim_{\mathbb{C}} M_1\ 个} \oplus \cdots \oplus \underbrace{X_s \oplus \cdots \oplus X_s}_{\dim_{\mathbb{C}} M_s\ 个}.$$

因为 $\dim_{\mathbb{C}} M_i = \deg X_i = \chi_i(1)$, 故取上式对应的特征标即可得到

$$r_G = \sum_{r=1}^{s} \chi_i(1)\chi_i.$$

□

定理 5.12 $e_i = \frac{1}{|G|} \sum_{a\in G} \chi_i(1)\chi_i(a^{-1})a$.

证 设 $e_i = \sum_{a\in G} \lambda_a a$, 我们要证明

$$\lambda_a = \frac{1}{|G|}\chi_i(1)\chi_i(a^{-1}). \tag{5.4}$$

固定一个 $a \in G$, 我们来计算 $r_G(e_i a^{-1})$. 由例 5.4 中 r_G 的表达式有

$$r_G(e_i a^{-1}) = \lambda_a |G|,$$

而由引理 5.9,

$$r_G(e_i a^{-1}) = \sum_{j=1}^{s} \chi_j(1)\chi_j(e_i a^{-1}).$$

于是

$$\lambda_a |G| = \sum_{j=1}^{s} \chi_j(1)\chi_j(e_i a^{-1}). \tag{5.5}$$

再考虑 G 的表示 χ_j, 把它看成 $\mathbb{C}[G]$ 的表示，有

$$X_j(e_i a^{-1}) = X_j(1)(e_i)X_j(a^{-1}) = \begin{cases} 0, & i \neq j \\ X_i(a^{-1}), & i = j. \end{cases}$$

因此对特征标也有

$$\chi_j(e_i a^{-1}) = \chi_i(a^{-1})\delta_{ij}.$$

代入 (5.5) 式得

$$\lambda_a |G| = \chi_i(1)\chi_i(a^{-1}),$$

(5.4) 式成立.

定理 5.13 (第一正交关系) 对任意的 $i, j = 1, \cdots, s$, 有

$$\frac{1}{|G|}\sum_{a\in G}\chi_i(a)\chi_j(a^{-1}) = \delta_{ij}.$$

证 考虑幂等元 $e_1, \cdots, e_s$ 有关系

$$1 = \sum_{i=1}^{s} e_i, \quad e_i \in M_i([G]),$$

于是

$$e_i e_j = \delta_{ij} e_i, \ \forall i, j.$$

把定理 5.10 中求得的 e_i 的表达式代入上式，并比较两边在 $a = 1$ 时的系数. 右边是 $\frac{1}{|G|}\delta_{ij}\chi_i(1)^2$, 而左边是

$$\frac{1}{|G|^2}\chi_i(1)\chi_j(1)\sum_{a\in G}\chi_i(a)\chi_j(a^{-1}).$$

于是

$$\frac{\chi_j(1)}{|G|}\sum_{a\in G}\chi_i(a)\chi_j(a^{-1}) = \delta_{ij}\chi_i(1).$$

当 $i=j$ 时即得到 $\frac{1}{|G|}\sum\limits_{a\in G}\chi_i(a)\chi_j(a^{-1})=1$. 而当 $i\neq j$ 时得到 $\frac{1}{|G|}\sum\limits_{a\in G}\chi_i(a)\chi_j(a^{-1})=0$. 统一起来即要证明的第一正交关系. □

由定理 5.5(6), $\chi_i(a^{-1})=\overline{\chi_i(a)}$, 于是上定理可改写为

定理 5.13′ (第一正交关系) 对任意的 $i,j=1,\cdots,s$, 有

$$\frac{1}{|G|}\sum_{a\in G}\chi_i(a)\overline{\chi_j(a)}=\delta_{ij}.$$

我们在 $Cf(G)$ 中如下规定内积: 设 $\varphi,\psi\in Cf(G)$, 则 φ,ψ 的内积 $\langle\varphi,\psi\rangle_G$ 为

$$\langle\varphi,\psi\rangle_G=\frac{1}{|G|}\sum_{a\in G}\varphi(a)\overline{\psi(a)}.$$

如果所考虑的问题只涉及一个群 G, 则 $\langle\varphi,\psi\rangle_G$ 常简记作 $\langle\varphi,\psi\rangle$. 容易验证.

定理 5.14 内积 $\langle\varphi,\psi\rangle$ 使 $Cf(G)$ 成为 $\mathbb{C}$ 上的 s 维 U-空间, 且 $\mathrm{Irr}(G)$ 是 $Cf(G)$ 的标准正交基.

证 易证 $\langle\varphi,\psi\rangle$ 满足

(1) $\langle\varphi,\psi\rangle=\overline{\langle\psi,\varphi\rangle}$;

(2) $\langle\varphi,\varphi\rangle\geq 0$, 且等号仅当 $\varphi=0$ 时成立;

(3) $\langle\lambda_1\varphi_1+\lambda_2\varphi_2,\psi\rangle=\lambda_1\langle\varphi_1,\psi\rangle+\lambda_2\langle\varphi_2,\psi\rangle$, $\lambda_1,\lambda_2\in\mathbb{C}$.

于是 $Cf(G)$ 是 $\mathbb{C}$ 上的 U-空间. 又由定理 5.13′, $\mathrm{Irr}(G)$ 是 $Cf(G)$ 的标准正交基. □

应用类函数的内积概念及命题 5.7 可得

推论 5.15 设 $\varphi\in Cf(G)$, 则 φ 是特征标 $\Longleftrightarrow$ $\langle\varphi,\chi_i\rangle$ 为非负整数, $i=1,\cdots,s$.

证 设 $\varphi = \sum_{i=1}^{s} \lambda_i \chi_i$. 与 χ_i 作内积即推得 $\lambda_i = \langle \varphi, \chi_i \rangle$. 再应用命题 5.9 即得所需结论. □

下面的推论也很重要, 其证明留给读者.

推论 5.16 (1) 若 χ, ψ 是 G 的特征标, 则 $\langle \chi, \psi \rangle$ 是非负整数;
(2) 特征标 χ 不可约 $\Longleftrightarrow \langle \chi, \chi \rangle = 1$.

由第一正交关系可推出下面的

定理 5.17 (第二正交关系) 设 $a, b \in G$, 则

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(a)\overline{\chi(b)} = \begin{cases} 0, & \text{如果 } a, b \text{ 不共轭}, \\ |C_G(a)|, & \text{如果 } a, b \text{ 共轭}. \end{cases}$$

证 设 $C_1, \cdots, C_s$ 是 G 的 s 个共轭元素类, 而 $a_1, \cdots, a_s$ 是它们的代表元. 令

$$\mathbf{M} = \begin{pmatrix} \chi_1(a_1) & \cdots & \chi_1(a_s) \\ \cdots & \cdots & \cdots \\ \chi_s(a_1) & \cdots & \chi_s(a_s) \end{pmatrix},$$

$$\mathbf{D} = \begin{pmatrix} |C_1| & & & 0 \\ & \ddots & & \\ & & \ddots & \\ 0 & & & |C_s| \end{pmatrix},$$

由第一正交关系, 对于 $i, j = 1, \cdots, s$, 有

$$\begin{aligned} |G|\delta_{ij} &= \sum_{a \in G} \chi_i(a)\overline{\chi_j(a)} \\ &= \sum_{k=1}^{s} |C_k| \chi_i(a_k)\overline{\chi_j(a_k)}. \end{aligned}$$

这 s^2 个式子可以统一为 $\mathbf{M}\mathbf{D}\overline{\mathbf{M}}' = |G|\mathbf{I}$, 其中 $\overline{\mathbf{M}}'$ 表示 $\mathbf{M}$ 的转置再取共轭. 因此 $\mathbf{D}\overline{\mathbf{M}}'$ 是 $\frac{1}{|G|}\mathbf{M}$ 的逆矩阵. 这样我们也有 $D\overline{\mathbf{M}}'\mathbf{M} = |G|\mathbf{I}$, 即

$$\sum_{k=1}^{s} |C_i| \overline{\chi_k(a_i)} \chi_k(a_j) = |G|\delta_{ij}.$$

因为 $|G|/|C_i| = |C_G(a_i)|$, 于是有

$$\sum_{k=1}^{s} \chi_k(a_j)\overline{\chi_k(a_i)} = |C_G(a_i)|\delta_{ij},$$

定理得证. □

在群论的实际应用中，常常需要造出给定群的特征标表，即给出上述矩阵 **M**. 造特征标表没有一般的方法，以下我们利用本节结果给出几个造特征标表的例子.

例 5.18 造对称群 S_3 的特征标表.

解 S_3 有三个共轭类，其代表为 1, (12), (123), 因此它有三个不可约特征标. 又因 $|S_3/S_3'| = |S_3/A_3| = 2$, 故 S_3 有两个线性特征标，而第三个特征标的级 $\chi_3(1)$ 由

$$\sum_{i=1}^{3} \chi_i(1)^2 = |S_3| = 6$$

来确定. 由计算知 $\chi_3(1) = 2$. 又线性特征标中有一个是主特征标，另一个诱导出 S_3/A_3 的非平凡表示，故必把偶置换映到 1, 奇置换映到 -1. 于是所求的特征标表为

	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	λ	μ

其中 λ, μ 待定. 在第二正交关系中令 $a = 1, b = (12)$, 于是得

$$\sum_{k=1}^{3} \chi_k(1)\overline{\chi_k((12))} = 0$$

即 $1 \cdot 1 + 1 \cdot (-1) + 2 \cdot \lambda = 0$, 从而推出 $\lambda = 0$. 再在第二正交关系中令 $a = 1, b = (123)$, 依同法可得 $\mu = -1$. 代入上表即完成了 S_3 的指标表. □

例 5.19 造交错群 A_4 的特征标表.

解：A_4 有 4 个共轭类，其代表元为 1, (12)(34), (123), (132), 故 A_4 有四个不可约特征标. 又因 $A_4' = V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$, $|A_4/V_4| = 3$. 故它有三个线性特征标，第四个特征标的级由 $\sum_{i=1}^{4} \chi_i(1)^2 = |A_4| = 12$ 可定出，即 $\chi_4(1) = 3$. A_4 的线性特征标对应于 3 阶循环群 A_4/V_4 的三个不可约表示，故可得 A_4 的特征标表为

	1	(12)(34)	(123)	(132)
χ_1	1	1	1	1
χ_2	1	1	$e^{\frac{2\pi i}{3}}$	$e^{\frac{-2\pi i}{3}}$
χ_3	1	1	$e^{\frac{-2\pi i}{3}}$	$e^{\frac{2\pi i}{3}}$
χ_4	3	λ	μ	ν

其中 λ, μ, ν 待定. 应用正交关系可算出 $\lambda = -1$, $\mu = \nu = 0$, 细节略. □

例 5.20 造 8 阶非交换群 G 的特征标表.

解：无论是 8 阶二面体群还是四元数群，都有五个共轭类，且都有 $|G/G'| = 4$, 故 G 有四个线性特征标 $\chi_1, \cdots, \chi_4$ 和一个二级特征标 χ_5. ($\chi_5(1) = 2$ 可由 $\sum_{k=1}^{5} \chi_k(1) = 8$ 算出). 因为 G/G' 是 (2,2) 型初等交换群，故其线性特征标为 G/G' 的四个不可约特征标. 因此它的特征标表为

	a_1	a_2	a_3	a_4	a_5
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	1	1	-1	-1	1
χ_4	1	-1	-1	1	1
χ_5	2	λ	μ	ν	θ

这里假定 $G' = \{a_1, a_5\}$, $a_1 = 1$. 最后由正交关系定出 $\theta = -2$, $\lambda = \mu = \nu = 0$. □

这个例子说明不同构的群可以有相同的特征标表. 因此, 特征标表所提供的关于群结构的信息是不完全的. 但是, 它还是能说明很多问题的. 譬如可由特征标表找出群 G 的所有正规子群, 因而亦可判断 G 是否为单群.

因为正规子群是由群的若干共轭类的并所组成, 所谓找出一个正规子群就是指出所有含于这个子群的共轭类. 对于 G 的任一不可约特征标 χ_i, $N_i = \text{Ker}\ \chi_i$ 是 G 正规子群, 而且共轭类 $C \subseteq N_i$ 的充要条件为对 C 中的代表元 a 有 $\chi_i(a) = \chi_i(1)$. 这样可由特征标表找出 s 个正规子群 $N_1, \cdots, N_s$, 它们是诸不可约表示的核. 下面我们证明, G 的任一正规子群都是若干个 N_i 的交, 这样就可找出 G 的所有正规子群了. 设 $N \trianglelefteq G$, 考虑 $\overline{G} = G/N$. $\overline{G}$ 的正则特征标 $r_{\overline{G}}$ 的核恰为 N. 但 $r_{\overline{G}}$ 作为 G 的特征标有表达式 $r_{\overline{G}} = \sum_{i=1}^{s} \lambda_i \chi_i$, 其中 λ_i 是非负整数, 易见

$$\text{Ker}\ r_{\overline{G}} = \bigcap_{\lambda_i \neq 0} \text{Ker}\ \chi_i,$$

这就证明了我们的断言.

§6. 诱导特征标

设 G 是有限群, $H \leq G$. 又设 $X : G \to GL(V)$ 是一表示, 其中 $V = V(n, \mathbb{C})$, 而 χ 是它的特征标. 则如果把 X 限制在 H 上, 也将得到 H 的一个表示. 我们记它为 $X|_H$. 并以 $\chi|_H$ 表示 $X|_H$ 的特征标.

本节考虑的问题恰与上述过程相反, 即如何由 H 的一个给定的特征标通过某种方法构造出 G 的一个特征标. 我们称它为 H 的特征标在 G 上的*诱导特征标*.

首先定义*诱导类函数*.

定义 6.1 设 $H \leq G$, $|H| = h$, $\varphi \in Cf(H)$ 是 H 到 $\mathbb{C}$ 上的一个类函数. 对于 $a \in G$, 令

$$\varphi^G(a) = \frac{1}{h} \sum_{t \in G} \varphi^0(tat^{-1}), \tag{6.1}$$

其中

$$\varphi^0(y) = \begin{cases} \varphi(y), & \text{如果 } y \in H, \\ 0, & \text{如果 } y \notin H. \end{cases} \tag{6.2}$$

我们称 φ^G 为 φ 在 G 上的诱导类函数.

容易看出，若 a 与 b 在 G 中共轭，譬如 $b = xax^{-1}$, 则

$$\begin{aligned} \varphi^G(b) &= \frac{1}{h}\sum_{t\in G}\varphi^0(tbt^{-1}) \\ &= \frac{1}{h}\sum_{t\in G}\varphi^0(txa(tx)^{-1}) \\ &= \frac{1}{h}\sum_{t\in G}\varphi^0(tat^{-1}) = \varphi^G(a). \end{aligned}$$

这说明 φ^G 确为 G 之类函数. 又由计算可得

$$\varphi^G(1) = |G:H|\varphi(1).$$

且若

$$G = Ht_1 \cup Ht_2 \cup \cdots \cup Ht_k$$

是 G 关于 H 的右陪集分解式，令 $T = \{t_1, \cdots, t_k\}$, 则有

$$\varphi^G(a) = \sum_{t\in T}\varphi^0(tat^{-1}). \tag{6.3}$$

例 6.2 设 r_H 是 H 的正则特征标，则 $(r_H)^G = r_G$.

证 因为

$$(r_H)^G(1) = |G:H|r_H(1) = |G:H||H| = |G|,$$

而若 $1 \neq a \in G$, 由 (6.3) 式,

$$(r_H)^G(a) = \sum_{t\in T} r_H^0(tat^{-1}) = 0.$$

于是由例 5.4, 有 $(r_H)^G = r_G$. □

由直接验证可得

命题 6.3 设 $\varphi_1,\cdots,\varphi_r \in Cf(H)$, $\lambda_1,\cdots,\lambda_r \in \mathbb{C}$, 则

$$\left(\sum_{i=1}^{r}\lambda_i\varphi_i\right)^G = \sum_{i=1}^{r}\lambda_i\varphi_i^G.$$

定理 6.4 (Frobenius 互反律) 设 $H \le G$, $|H| = h$, $|G| = g$. 又设 $\varphi \in Cf(H)$, $\psi \in Cf(G)$, 则

$$\langle\varphi^G,\psi\rangle_G = \langle\varphi,\psi|_H\rangle_H.$$

证 因为

$$\begin{aligned}\langle\varphi^G,\psi\rangle_G &= \frac{1}{g}\sum_{a\in G}\varphi^G(a)\overline{\psi(a)}\\ &= \frac{1}{g}\sum_{a\in G}\left(\frac{1}{h}\sum_{t\in G}\varphi^0(tat^{-1})\overline{\psi(a)}\right),\end{aligned}$$

其中 $g=|G|$, 而 $tat^{-1}\in H$ 当且仅当 $a\in t^{-1}Ht$, 故

$$\begin{aligned}\langle\varphi^G,\psi\rangle_G &= \frac{1}{g}\sum_{t\in G}\left(\frac{1}{h}\sum_{a\in t^{-1}Ht}\varphi^0(tat^{-1})\overline{\psi(tat^{-1})}\right)\\ &= \frac{1}{g}\sum_{t\in G}\left(\frac{1}{h}\sum_{y\in H}\varphi(y)\overline{\psi(y)}\right)\\ &= \frac{1}{g}\sum_{t\in G}\langle\varphi,\psi|_H\rangle_H = \langle\varphi,\psi|_H\rangle_H.\end{aligned}$$

□

推论 6.5 设 $H\le G$, φ 是 H 的特征标, 则 φ^G 也是 G 的特征标.

证 作为 G 的类函数, 可令

$$\varphi^G = \sum_{i=1}^{s}\lambda_i\chi_i,$$

其中 $\chi_1, \cdots, \chi_s$ 是 G 的全部不可约特征标. 为证 φ^G 是特征标, 只须证 λ_i 为非负整数且 φ^G 不是零函数. 由定理 6.4,

$$\lambda_i = \langle \varphi^G, \chi_i \rangle_G = \langle \varphi, \chi_i|_H \rangle_H.$$

因为 $\varphi, \chi_i|_H$ 皆为 H 的特征标, 故 $\langle \varphi, \chi_i|_H \rangle_H$ 为非负整数, 这样 λ_i 亦为非负整数. 最后, 因为

$$\varphi^G(1) = |G : H|\varphi(1) \neq 0,$$

故 φ^G 不是零函数. □

事实上, 诱导特征标所对应的表示也可由子群 H 的表示得到, 但要用到表示的张量积的概念, 这里就不叙述了. 有兴趣的读者可参 C.W. Curtis 和 I. Reiner 著 "Representation Theory of Finite Groups and Associative Algebras" 一书.

诱导特征标对于构造有限群的特征标表是一个有用的工具. 因为一个群纵然很复杂, 但它总有很多简单的子群, 这些子群的特征标表容易造出, 于是用诱导特征标的理论就可得到原来群的若干特征标. 下面我们看一个例子, 即造交错群 A_5 的特征标表. 为了便于计算诱导特征标, 我们先给出下面的计算公式.

命题 6.6 *设 $H \leq G$, $\varphi \in Cf(H)$, $a \in G$. 以 $C(a)$ 表示 G 中包含 a 的共轭类, 则 $H \cap C(a)$ 由 H 的若干共轭类的并组成. 设 $x_1, \cdots, x_m$ 是这些共轭类的代表元, 则*

$$\varphi^G(a) \quad |C_G(a)| \sum_{i=1}^{m} \frac{\varphi(x_i)}{|C_H(x_i)|}; \tag{6.4}$$

而若 $H \cap C(a) = \varnothing$, 则 $\varphi^G(\ ) = 0$.

证 若 $H \cap C(a) = \varnothing$, 由 (6.1) 式显然 $\varphi^G(a) = 0$, 故下面设 $H \cap C(a) \neq \varnothing$. 因为对于某个 $t_0 a t_0^{-1} \in H$, 恰有 $C_G(a)$ 个 G 的元素 t 使 $tat^{-1} = t_0 a t_0^{-1}$, 于是据 (6.1) 式有

$$\begin{aligned} \varphi^G(a) &= \frac{1}{h} \sum_{t \in G} \varphi^0(tat^{-1}) \\ &= \frac{1}{h} |C_G(a)| \sum_{y \in H \cap C(a)} \varphi(y), \end{aligned}$$

其中 $h=|H|$. 又对 $x_i\in H\cap C(a)$, 恰有 $\frac{h}{|C_H(x_i)|}$ 个与 x_i 在 H 中共轭的元素属于 $H\cap C(a)$, 故上式变为

$$\begin{aligned}\varphi^G(a) &= \frac{1}{h}|C_G(a)|\sum_{i=1}^{m}\frac{h}{|C_H(x_i)|}\varphi(x_i)\\ &= |C_G(a)|\sum_{i=1}^{m}\frac{\varphi(x_i)}{|C_H(x_i)|}.\end{aligned}$$

□

例 6.7 造 A_5 的特征标表.

解: A_5 有五个共轭类, 阶为 1, 2, 3 的元素各有一类, 而 5 阶元素有两个共轭类. 为方便起见, 记这五类为 $C_1,C_2,C_3,C_5^{(1)},C_5^{(2)}$. 各类的长度及代表元中心化子的阶列表如下:

类C	C_1	C_2	C_3	$C_5^{(1)}$	$C_5^{(2)}$
$\lvert C\rvert$	1	15	20	12	12
$\lvert C_G(a)\rvert, a\in C$	60	4	3	5	5

A_5 有五个不可约特征标 $\chi_1,\cdots,\chi_5$, 其中 χ_1 是主特征标, 在各共轭类上取值依次为

$$\chi_1: \quad 1 \quad 1 \quad 1 \quad 1 \quad 1$$

设 $H=A_4\le A_5$, 用命题 6.6 可算出 (过程从略):

$$(1_H)^G: \quad 5 \quad 1 \quad 2 \quad 0 \quad 0$$

因为 $\langle(1_H)^G,1_G\rangle_G=\langle 1_H,1_H\rangle_H=1$, 故 $(1_H)^G-1_G=\chi_2$ 也是 G 的特征标:

$$\chi_2: \quad 4 \quad 0 \quad 1 \quad -1 \quad -1$$

直接计算得 $\langle\chi_2,\chi_2\rangle=1$, 于是 χ_2 是一不可约特征标. 再由 A_4 的另一线性特征标 λ (即例 5.19 中的 χ_2) 出发, 计算 λ^G 得:

$$\lambda^G: \quad 5 \quad 1 \quad -1 \quad 0 \quad 0$$

直接计算知 $\langle\lambda^G,\lambda^G\rangle=1$, 于是 λ^G 亦为 G 之不可约特征标. 命 $\lambda^G=\chi_3$. (注意, 若由 A_4 的第二个线性特征标, 即例 5.19 中的 χ_3, 出发计算诱导特征标, 仍将得到 χ_3, 因此为得到新特征标还要想其他办法.)

再取 A_5 的一个五阶子群 $K=\langle x\rangle$. 易验证 x,x^{-1} 和 x^2,x^{-2} 分属 A_5 的两个不同的共轭类 $C_5^{(1)}$ 和 $C_5^{(2)}$. 令 μ 是 K 的线性特征标满足 $\mu(x)=\varepsilon=e^{2\pi i/5}$ 者. 计算 μ^G 得

$$\mu^G:\quad 12\quad 0\quad 0\quad \varepsilon+\varepsilon^4\quad \varepsilon^2+\varepsilon^3.$$

再由计算可得 $\langle\mu^G,\chi_2\rangle=1$, $\langle\mu^G-\chi_2,\chi_3\rangle=1$. 于是 $\mu^G-\chi_2-\chi_3=\chi_4$ 也是 G 的特征标:

$$\chi_4:\quad 3\quad -1\quad 0\quad \varepsilon+\varepsilon^4+1\quad \varepsilon^2+\varepsilon^3+1$$

且因 $\langle\chi_4,\chi_4\rangle=1$, 故 χ_4 是 G 的不可约特征标, 至此我们已找到 A_5 的四个不可约特征标. 第五个可用正交关系算出, 即

$$\chi_5:\quad 3\quad -1\quad 0\quad \varepsilon^2+\varepsilon^3+1\quad \varepsilon+\varepsilon^4+1$$

于是最终完成了 A_5 的特征标表如下

类C	C_1	C_2	C_3	$C_5^{(1)}$	$C_5^{(2)}$
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3	-1	0	$\varepsilon+\varepsilon^4+1$	$\varepsilon^2+\varepsilon^3+1$
χ_5	3	-1	0	$\varepsilon^2+\varepsilon^3+1$	$\varepsilon+\varepsilon^4+1$

§7. 有关代数整数的预备知识

为了进一步研究特征标的性质, 也为了满足下一节的需要, 本节将叙述代数数论方面的一些预备知识, 对于抽象代数知识较多的读者, 本节的大部分内容是熟知的.

定义 7.1 复数 a 称为 代数整数, 如果它是某首项系数为 1 的整系数多项式的零点.

通常意义下的整数, 以后称为有理整数, 以强调它们与代数整数的区别.

自然, 有理整数都是代数整数, 我们还有:

定理 7.2 如果有理数 a 是代数整数, 则它必是有理整数.

证 设 $a=\frac{b}{c}$, 其中 b,c 是有理整数, $c>0$, $(b,c)=1$. 并设 a 是多项式

$$x^n+a_1x^{n-1}+\cdots+a_n$$

的零点, 其中 $a_1,\cdots,a_n$ 是有理整数. 于是

$$\frac{b^n}{c^n}+a_1\frac{b^{n-1}}{c^{n-1}}+\cdots+a_n=0,$$

即

$$b^n=-a_1b^{n-1}c-\cdots-a_nc^n.$$

于是 $c|b^n$, 但 $(b,c)=1$, 所以 $c=1$, a 是有理整数. □

定理 7.3 复数 a 是代数整数, 当且仅当存在复数域的子环 $R\supseteq\mathbb{Z}$, 使得 $a\in R$, 且 R 的加法群是有限生成的.

证 设 a 是代数整数, 则 a 是有理整系数多项式 $x^n+a_1x^{n-1}+\cdots+a_n$ 的零点. 命

$$R=\left\{\sum_{i=0}^{n-1}b_ia^i \mid b_i\in\mathbb{Z},\ i=0,1,\cdots,n-1\right\},$$

则 R 是 $\mathbb{C}$ 的子环, 包含 $\mathbb{Z}$, 且 R 的加法群由 $1,a,\cdots,a^{n-1}$ 生成.

反之, 设复数域的子环 $R\supseteq\mathbb{Z}$, 且 R 的加法群由 $e_1,\cdots,e_n$ 生成, $a\in R$. 那么存在整系数矩阵 $\mathbf{A}$ 满足

$$a\begin{pmatrix}e_1\\ \vdots\\ e_n\end{pmatrix}=\mathbf{A}\begin{pmatrix}e_1\\ \vdots\\ e_n\end{pmatrix},$$

即

$$(a\mathbf{I}-\mathbf{A})\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

两边同乘 $a\mathbf{I}-\mathbf{A}$ 的伴随矩阵，得

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = |a\mathbf{I}-\mathbf{A}|\cdot\mathbf{I}\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} |a\mathbf{I}-\mathbf{A}|\cdot e_1 \\ \vdots \\ |a\mathbf{I}-\mathbf{A}|\cdot e_n \end{pmatrix}.$$

由 $e_1,\cdots,e_n$ 不全为 0 (因为 $R\neq 0$), 所以 $|a\mathbf{I}-\mathbf{A}|=0$, 即 a 是首项系数为 1 的整系数多项式 $|\lambda\mathbf{I}-\mathbf{A}|$ 的零点. □

设 a, b 是两个代数整数，由定理 7.3 可设它们分别属于复数域的子环 R_1, R_2, 其中

$$R_1=\left\{\sum_{i=1}^{m}a_ie_i \mid a_i\in\mathbb{Z}\right\},$$

$$R_2=\left\{\sum_{j=1}^{n}b_jf_j \mid b_j\in\mathbb{Z}\right\},$$

并可设 $e_1=f_1=1$, 那么显然有

$$R=\left\{\sum_{i=1}^{m}\sum_{j=1}^{n}c_{ij}e_if_j \mid c_{ij}\in\mathbb{Z}\right\}$$

也是 $\mathbb{C}$ 的子环，且 $R\ni a+b$, $a-b$ 和 ab, 所以有

定理 7.4 代数整数的和差积仍是代数整数，即 $\mathbb{C}$ 中全体代数整数组成一环.

根据这个定理和定理 5.5(5), 我们立即看出 $\chi(t)$ 恒是代数整数，其中 χ 是 G 的特征标， $t\in G$.

下面我们举出另一个恒取代数整数值的类函数的例子.

设 C_i, C_j 为群 G 的任二共轭类，命

$$C_iC_j = \{xy \mid x \in C_i, y \in C_j\}.$$

对于任意的 $xy \in C_iC_j$ 和 $t \in G$, 有

$$(xy)^t = x^t y^t \in C_iC_j,$$

这说明 C_iC_j 仍为 G 之若干共轭类之并. 假设又有 $x_1y_1 = xy$, 其中 $x_1 \in C_i, y_1 \in C_j$, 则 $x_1^t y_1^t = x^t y^t = (xy)^t$, 并且若 $x_1 \neq x$ 或 $y_1 \neq y$, 亦有 $x_1^t \neq x^t$ 或 $y_1^t \neq y^t$. 这说明对 C_iC_j 中的任二共轭元素 xy 和 $(xy)^t$, 在表示成一个 C_i 的元素和一个 C_j 的元素之乘积时，表示方法也有同样多个. 利用这点我们可以证明

定理 7.5 设 χ 是 G 的不可约复特征标，对于 $t \in G$ 规定

$$\omega(t) = \frac{|C|\chi(t)}{\chi(1)},$$

其中 C 为 t 所在的共轭元素类. 则 ω 是 G 类函数，且取值为代数整数.

证 设 $\mathbf{X}$ 是 χ 对应的不可约矩阵表示. 令

$$\mathbf{Z}(t) = \sum_{c \in C} \mathbf{X}(c).$$

易验证 $\mathbf{Z}(t)$ 与所有 $\mathbf{X}(a)$ 可交换， $a \in G$. 由 Schur 引理，存在复数 λ 使

$$\mathbf{Z}(t) = \lambda \mathbf{I}.$$

于是

$$\lambda\chi(1) = \mathrm{tr}\ (\mathbf{Z}(t)) = \sum_{c \in C} \mathrm{tr}\ (\mathbf{X}(t)) = \sum_{c \in C} \chi(c) = |C|\chi(t),$$

所以

$$\lambda = \frac{|C| \cdot \chi(t)}{\chi(1)} = \omega(t).$$

由本定理前面的讨论，对任意的 $x,y\in G$，我们有

$$\mathbf{Z}(x)\cdot\mathbf{Z}(y)=\sum_t a_t\mathbf{Z}(t),$$

其中 t 遍取 G 的共轭类代表．a_t 是非负整数，但 $\mathbf{Z}(t)$ 都是纯量阵，由此有

$$\omega(x)\cdot\omega(y)=\sum_t a_t\omega(t).$$

这样，$\{\sum a_t\omega(t)\mid a_t\in\mathbb{Z}\}$ 是 $\mathbb{C}$ 的一个子环，从而 $\omega(t)$ 为代数整数． □

推论 7.6 设 χ 是 G 的一个不可约特征标，则 $\chi(1)|g$，其中 $g=|G|$．

证 设 $C_i, i=1,\cdots,s$，是 G 的全部共轭类，$t_i\in C_i$，则

$$\begin{aligned}\frac{g}{\chi(1)} &= \frac{g}{\chi(1)}\langle\chi,\chi\rangle\\ &= \frac{g}{\chi(1)}\cdot\frac{1}{g}\sum_{i=1}^{s}|C_i|\chi(t_i)\overline{\chi(t_i)}\\ &= \sum_{i=1}^{s}\frac{|C_i|\chi(t_i)}{\chi(1)}\overline{\chi(t_i)}\\ &= \sum_{i=1}^{s}\omega(t_i)\overline{\chi(t_i)}.\end{aligned}$$

所以 $g/\chi(1)$ 是代数整数．又因它是有理数，故为有理整数，即 $\chi(1)|g$． □

最后，我们来讨论有理数域上的分圆多项式．

我们知道，在复数域中，只有 $\varphi(n)$ 个 n 次本原单位根，其中 φ 是 Euler φ 函数．以 $\zeta_1,\cdots,\zeta_{\varphi(n)}$ 记这 $\varphi(n)$ 个 n 次原根，称多项式

$$f_n(x)=\prod_{i=1}^{\varphi(n)}(x-\zeta_i)$$

为 n 次分圆多项式. 容易验证

$$x^n-1=\prod_{d|n} f_d(x),$$

上式右边是对 n 的所有正因子 d 取乘积，这样 $f_n(x)$ 必是首 1 有理整系数多项式. 这是因为: $f_1(x)=x-1$, 是首 1 有理整系数的; 对 n 施行归纳法，设 $f_d(x), d<n$, 全是首 1 有理整系数的，则

$$f_n(x)=\frac{x^n-1}{\prod_{d|n,d<n} f_d(x)}=\frac{x^n-1}{g(x)}.$$

因为 $g(x)$ 是首 1 有理整系数的，且 $g(x)|x^n-1$, 由带余除法可以看出 $f_n(x)$ 也是首 1 有理整系数多项式.

定理 7.7 *$f_n(x)$ 在有理数域 $\mathbb{Q}$ 上不可约.*

证 设 $f_n(x)$ 在有理数域 $\mathbb{Q}$ 上有分解

$$f_n(x)=g(x)h(x),$$

其中 $g(x)$ 的次数 ≥ 1. 由 Gauss 关于本原多项式的引理，不失普遍性，可设 $g(x), h(x)$ 是有理整系数的，因而是首 1 的. 设 ζ 是 $g(x)$ 的一个零点，我们证明，对每一满足 $p\nmid n$ 的素数 p, ζ^p 仍是 $g(x)$ 的零点，于是 $g(x)$ 将以任一 n 次原根为其零点，这推出 $g(x)=f_n(x)$, 即可完成定理的证明.

设其不然，由于 ζ^p 仍是原根，所以 ζ^p 是 $h(x)$ 的零点，即 $g(x)$ 与 $h(x^p)$ 有一公共零点，也即 $g(x)$ 与 $h(x^p)$ 不互素.

用 $\bar{f}(x)$ 表示把整系数多项式 $f(x)$ 的系数分别换成其模 p 的同余类而得到的 Galois 域 $GF(p)$ 上的多项式, 则显然有 $f(x)\mapsto\bar{f}(x)$ 是 $\mathbb{Z}[x]$ 到 $GF(p)[x]$ 上的同态. 于是 $\bar{g}(x)$ 与 $\bar{h}(x^p)$ 仍不互素, 从而 $\bar{g}(x)$ 与 $\bar{h}(x)$ 不互素. 但 $\bar{g}(x)\cdot\bar{h}(x)=\bar{f}_n(x)$ 是 x^n-1(看作 $GF(p)$ 上多项式) 的因子，而 $p\nmid n$, 所以 x^n-1 无重零点，此系矛盾. □

推论 7.8 *设 ζ_1,ζ_2 都是 n 次本原单位根，则有理数域 $\mathbb{Q}$ 的扩域 $\mathbb{Q}(\zeta_1)$ 有一自同构把 ζ_1 变到 ζ_2.*

证 由于 ζ_1 和 ζ_2 同是不可约多项式 $f_n(x)$ 的零点，所以存在同构 $\sigma: \mathbb{Q}(\zeta_1) \to \mathbb{Q}(\zeta_2)$ 满足 $\zeta_1^\sigma = \zeta_2$, 但 $\mathbb{Q}(\zeta_1) = \mathbb{Q}(\zeta_2)$, 所以 σ 是自同构. □

§8. p^aq^b-定理, Frobenius 定理

前面介绍的特征标理论，在本节中获得出色的应用. 我们将在本节证明前面提到的 p^aq^b-定理以及 Frobenius 定理.

定理 8.1 设 χ 是 G 的一个不可约特征标, C 是 G 的一个共轭类, $x \in C$. 若 $(\chi(1), |C|) = 1$, 则或者 $\chi(x) = 0$, 或者 $|\chi(x)| = \chi(1)$.

证 因为 $(\chi(1), |C|) = 1$, 必有整数 u, v 使 $u\chi(1) + v|C| = 1$, 于是

$$\begin{aligned}\frac{\chi(x)}{\chi(1)} &= \frac{(u\chi(1) + v|C|)\chi(x)}{\chi(1)} \\ &= v\omega(x) + u\chi(x),\end{aligned}$$

其中 ω 如定理 7.5 中定义，于是 $\chi(x)/\chi(1)$ 是代数整数.

令 $\chi(1) = k$, $o(x) = n$. 以 $\zeta_1, \cdots, \zeta_{\varphi(n)}$ 表 $\varphi(n)$ 个 n 次本原单位根，令 $a_1 = \chi(x)/\chi(1)$. 由定理 5.5(5) 可设

$$a_1 = (\zeta_1^{i_1} + \cdots + \zeta_1^{i_k})/k,$$

其中 $i_1, \cdots, i_k$ 是非负整数. 令 $a_j = (\zeta_j^{i_1} + \cdots + \zeta_j^{i_k})/k$, $j = 1, \cdots, \varphi(n)$. 由定理 7.8 有 $\mathbb{Q}(\zeta_1)$ 的自同构把 a_1 变到 a_j, 所以 a_j 亦是代数整数. 因为

$$\prod_{j=1}^{\varphi(n)} a_j = b$$

是 $\zeta_1, \cdots, \zeta_{\varphi(n)}$ 的对称多项式，因而可表成 $\zeta_1, \cdots, \zeta_{\varphi(n)}$ 的初等对称多项式即 $f_n(x)$ 的系数的有理函数，这推出 b 是有理数，但它又是代数整数，所以它是有理整数.

如果 $|\chi(x)| < \chi(1)$, 则 $|a_1| < 1$. 我们又有 $|a_j| \leq 1$, $j = 2,\cdots,\varphi(n)$. 于是有

$$|b| = |\prod_{j=1}^{\varphi(n)} a_j| < 1,$$

由此只能成立 $b = 0$, 于是 $a_1 = \chi(x)/\chi(1) = 0$, 即 $\chi(x) = 0$. □

定理 8.2 有限单群的共轭类的长度不能是素数的正方幂.

证　设 G 是有限单群, C 是 G 的一个共轭类. 又设 $|C| = p^a$, p 是素数, a 是正整数. 当然有 $p \mid |G|$, 且 G 是非交换的.

因为 $|G| = \sum_{i=1}^{s} \chi_i(1)^2$, 而 χ_1 是主特征标, 有 $\chi(1) = 1$, 所以至少有一个不可约特征标 χ 满足 $\chi \neq \chi_1$ 且 $p \nmid \chi(1)$. 不妨设 $p \nmid \chi_i(1)$, $i = 1,\cdots,r$ 但 $p \mid \chi_j(1)$, $j = r+1,\cdots,s$, 其中 $2 \leq r \leq s$. 若对某一 χ_i, $2 \leq i \leq r$, 有 $|\chi_i(x)| = \chi_i(1)$, $x \in C$. 令 $\mathbf{X}_i$ 是 χ_i 之相应的表示, 由定理 5.5(7) $\mathbf{X}_i(x)$ 是纯量阵. 而因 G 是单群, 所以 χ_i 是忠实的, 于是 G 的中心 $Z(G) \ni x$, 但这与 G 是非交换单群矛盾. 因此必有

$$\chi_i(x) = 0,\ x \in C,\ i = 2,\cdots,r.$$

由第二正交关系, 我们有: 对 $x \in C$,

$$\begin{aligned} 0 &= \sum_{i=1}^{s} \chi_i(1)\chi_i(x) \\ &= 1 + \sum_{j=r+1}^{s} \chi_j(1)\chi_j(x), \end{aligned}$$

注意到对 $j = r+1,\cdots,s$, $p \mid \chi_j(1)$, 我们有

$$1/p = -\sum_{j=r+1}^{s} \frac{\chi_j(1)}{p}\chi_j(x)$$

是代数整数, 因而也是有理整数, 矛盾. □

定理 8.3 (Burnside) p^aq^b 阶群必可解, 其中 p,q 是不同素数, a,b 是正整数.

证 设 G 是使定理不成立的最小阶反例, 则 G 应为单群. (若否, G 有非平凡正规子群 N, 则由 G 的最小性, 有 N 及 G/N 均可解, 于是 G 亦可解.) 令 $P \in \mathrm{Syl}_p(G)$, $1 \neq z \in Z(P)$, 则 z 所在的共轭类的长度必为 q 的方幂, 与定理 8.2 矛盾. □

下面, 我们讨论所谓 Frobenius 群, 并证明著名的 Frobenius 定理.

定义 8.4 设 G 是 $\Omega = \{1, \cdots, n\}$ 上的传递置换群, 它对点 1 的稳定子群 $G_1 \neq 1$, 但只有单位元素才有两个以上不动点, 这时称 G 为 Frobenius 群. G 中变动每个点的元素称为正则元素.

设 G 是如上定义的 Frobenius 群, 由 G 之传递性, 稳定子群 $G_2, \cdots, G_n$ 亦非单位群, 并且对任意的 $i \neq j$ 恒有 $G_i \cap G_j = 1$. 令 $H = G_1$, $|H| = h$, 则 $|G| = g = nh$. 因此 G 的正则元的个数为

$$\left| G - \bigcup_{i=1}^{n} G_i \right| = g - (h-1)n - 1 = n - 1,$$

而非正则元个数为 $(h-1)n$. 又, 对任一 $i \neq 1$, H 对点 i 的稳定子群 $H_i = 1$, 从而 H 的包含 i 的轨道 i^H 的长为 h. 因此, $h \mid n-1$. 特别地, $(n,h) = 1$.

定理 8.5 (Frobenius) Frobenius 群 G 中的正则元素和 1 一起组成 G 的一个特征子群.

证 保持前面所用的记号, 由于 $g = nh$, 而 $(n,h) = 1$, 所以如果能证明全体正则元和 1 组成 G 的正规子群, 则此子群当然是特征子群.

设 ρ 是 G 的置换特征标 (参看例 5.3), 则 $\rho(1) = n$, $\rho(x) = 0$, $\rho(y) = 1$, 其中 x 是任一正则元素, 而 y 是任一非正则元素. 计算可得 $\langle \rho, 1_G \rangle = \frac{1}{g}(n + (h-1)n) = 1$, 故若令 $\theta = \rho - 1_G$, 则 θ 仍

为 G 之特征标. 对 θ 有 $\theta(1)=n-1$, $\theta(x)=-1$, $\theta(y)=0$. 我们再令 $\mu=r_G-h\theta$, 其中 r_G 是 G 的正则特征标. 由计算可得, $\mu(1)=\mu(x)=h$, $\mu(y)=0$, 其中 x,y 如前所述. 如果我们能证明 μ 也是 G 的特征标, 由定理 5.5(7), Ker μ 将由正则元和 1 组成. 因为 Ker $\mu\trianglelefteq G$, 定理就证明完了.

为了证明 μ 是特征标, 我们设 $\psi_i, i=1,\cdots,t$, 是 H 的全部不可约特征标, 并设 $\psi_i(1)=m_i$, 于是有

$$r_H=\sum_{i=1}^{t}m_i\psi_i,\qquad \sum_{i=1}^{t}m_i^2=h.$$

又由例 6.2 有 $r_G=(r_H)^G$, 于是

$$\begin{aligned}\mu &= r_G-h\theta=(r_H)^G-h\theta\\ &= \left(\sum_{i=1}^{t}m_i\psi_i\right)^G-\left(\sum_{i=1}^{t}m_i^2\right)\theta\\ &= \sum_{i=1}^{t}m_i(\psi_i^G-m_i\theta).\end{aligned}$$

因此只须证明 $\pi_i=\psi_i^G-m_i\theta$ 是 G 的特征标. 由命题 6.6 易算出 $\psi_i^G(1)=nm_i$, $\psi_i^G(x)=0$, $\psi_i^G(y)=\psi_i(\bar{y})$, x,y 仍如前述, 而 $\bar{y}\in H$, 且与 y 在 G 中共轭. 又因 θ 的取值为 $\theta(1)=n-1$, $\theta(x)=-1$, $\theta(y)=0$, 由计算得

$$\pi_i(1)=m_i,\quad \pi_i(x)=m_i,\quad \pi_i(y)=\psi_i(\bar{y}),$$

并且

$$\begin{aligned}\langle\pi_i,\pi_i\rangle &= \frac{1}{g}\left(m_i^2+(n-1)m_i^2+n\sum_{\bar{y}\in H}\psi_i(\bar{y})\overline{\psi_i(\bar{y})}\right)\\ &= \frac{n}{g}\sum_{\bar{y}\in H}\psi_i(\bar{y})\overline{\psi_i(\bar{y})}\quad (\text{用到}m_i=\psi_i(1))\\ &= \langle\psi_i,\psi_i\rangle=1.\end{aligned}$$

又因 $\pi_i = \psi_i^G - m_i\theta$ 可表成 G 的不可约特征标的整系数线性组合，可令 $\pi_i = \sum_{i=1}^{s} \lambda_i\chi_i$，其中 λ_i 是整数，于是

$$\begin{aligned}\langle \pi_i, \pi_i \rangle &= \left\langle \sum_i \lambda_i\chi_i, \sum_i \lambda_i\chi_i \right\rangle \\ &= \sum_{i=1}^{s} \lambda_i^2 \langle \chi_i, \chi_i \rangle \\ &= \sum_{i=1}^{s} \lambda_i^2,\end{aligned}$$

这推出 $\sum_{i=1}^{s} \lambda_i^2 = 1$. 因此只有某一个 $\lambda_j = \pm 1$, 其余的 $\lambda_k = 0$. 于是 $\pi_i = \pm\chi_i$. 最后，因为 $\pi_i(1) = m_i > 0$, 必有 $\pi_i = \chi_j$，是 G 的不可约特征标. 定理证毕. □

习 题

注意，由于本章较初版有较大改动，特别是增加了群代数和半单代数的内容，将增加一部分习题. 为了与初版题号一致，我们把新增加的习题放在后面，即从 30 题开始.

1. 设 X 是群 G 的一个表示. 则映射

$$\det X : a \mapsto \det X(a),\ a \in G,$$

其中 $\det X(a)$ 表线性变换 $X(a)$ 的行列式，也是 G 的表示.

2. 设 $G = \langle a, b \rangle$ 是 $2n$ 阶二面体群，有定义关系：

$$a^n = 1,\ b^2 = 1,\ b^{-1}ab = a^{-1}.$$

又设 ε 是复数域上的 n 次本原单位根. 则映射

$$\mathbf{X} : a^i b^j \mapsto A^i B^j,\ i = 1, \cdots, n;\ j = 1, 2$$

是 G 的一个忠实不可约矩阵表示，其中

$$A = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

3. 证明例 1.7 中给出的群 G 的置换表示 $\mathbf{P}$ 是可约的，只要 $n \geq 2$.

4. 设 $\mathbf{X}$ 是 G 的任一非主不可约矩阵表示，则 $\sum_{a\in G}\mathbf{X}(a)=0$.

5. 设 $G=S_3$. 试把 G 的置换表示表成不可约表示的直和，从而得到 S_3 的一个二级不可约复表示.

6. 设 G 是有限交换群，以 G^* 记 G 的全部不可约复表示的集合. 规定 G^* 内的乘法如下：对 $X_1, X_2 \in G^*$，令

$$(X_1X_2)(a)=X_1(a)X_2(a),\ a\in G.$$

则 G^* 对此乘法成一群. 并证明：

(1) $G^*\cong G$;

(2) 对于 G 的任一子群 H，规定

$$H^d=\{X\in G^* \mid H\le \operatorname{Ker} X\}.$$

证明 $H^d\le G^*$，且映射 $H\mapsto H^d$ 是 G 的子群集合到 G^* 的子群集合间的一一对应，满足

$$H_1\ge H_2 \iff H_1^d\le H_2.$$

7. 设 χ 是群 G 的特征标，σ 是复数域 $\mathbb{C}$ 的自同构. 定义

$$\chi^\sigma(a)=(\chi(a))^\sigma,\ \forall a\in G.$$

求证 χ^σ 也是 G 的特征标，且 χ^σ 不可约当且仅当 χ 不可约，χ^σ 忠实当且仅当 χ 忠实.

8. 设 χ, ψ 是群 G 的特征标. 规定

$$(\chi\psi)(a)=\chi(a)\psi(a),\ \forall a\in G,$$

则 $\chi\psi$ 也是群 G 的特征标. 并且有

(1) 若 $\psi(1)=1$，则 $\chi\psi$ 不可约当且仅当 χ 不可约;

(2) 若 $\psi=\overline{\chi}$，且 $\chi(1)>1$，则 $\chi\psi$ 可约.

9. 设 χ 是群 G 的忠实特征标，$H\le G$. 求证 H 是交换的当且仅当 $\chi|_H$ 可表成 H 的线性特征标的和.

10. (1) 设 χ 是交换群 A 的特征标，则

$$\sum_{a\in A}|\chi(a)|^2\ge |A|\cdot\chi(1);$$

(2) 设 A 是群 G 的交换子群，χ 是 G 的不可约特征标，则 $\chi(1)\le |G:A|$.

11. 单群没有二级不可约特征标.

12. 若 G' 是非交换单群，则 G 没有 2 级不可约特征标.

13. 设 $a \in G$. 证明 a 与 a^{-1} 在 G 中共轭的充要条件是对 G 的所有特征标 χ, 恒有 $\chi(a)$ 是实数.

14. 称满足上题条件的元素 a 为 G 的实元素, 证明 G 中存在非单位的实元素当且仅当 G 的阶为偶数.

15. 设 $H \leq G$, χ 是 G 的忠实不可约特征标, 且 $\chi|_H$ 是 H 的不可约特征标. 则 $C_G(H) = Z(G)$.

16. 设 χ 是群 G 的特征标, 满足

$$\chi(a) = 0 \ , \forall a \neq 1,$$

则 $|G| \bigm| \chi(1)$.

17. 设 χ 是 G 的不可约特征标, $A \neq 1$ 是 G 的交换子群, 且 $\chi(1) = |G : A|$. 则

(1) $\chi(a) = 0$, $\forall a \in G - A$;

(2) A 中包含 G 的非平凡交换正规子群.

18. 设 $H, K \leq G$, $HK = G$. 又设 φ 是 H 的一个类函数. 证明 $\varphi^G|_K = (\varphi|_{H\cap K})^K$.

19. 设 $H \leq G$, φ 是 H 的类函数, ψ 是 G 的类函数. 证明 $(\varphi\cdot\psi|_H)^G = \varphi^G\psi$. (两个类函数 φ_1, φ_2 的乘积如下定义: $(\varphi_1\varphi_2(a) = \varphi_1(a)\varphi_2(a)$, $\forall a \in G$.)

20. 设 $b(G) = \max\{\chi(1) \bigm| \chi \in \mathrm{Irr}(G)\}$. 若 $H \leq G$, 则

$$b(H) \leq b(G) \leq |G : H| b(H).$$

21. 设 $H \trianglelefteq G$, $G = \bigcup_{i=1}^m Ht_i$ 是 G 对 H 的右陪集分解式. 又设 ψ 是 H 的特征标. 则对 $i = 1, \cdots, m$, 由

$$\psi_i(h) = \psi(t_i h t_i^{-1}), \ \forall h \in H$$

确定之 ψ_i 亦为 H 之特征标, 且

$$\psi^G|_H = \psi_1 + \psi_2 + \cdots + \psi_m.$$

22. 设 $H \trianglelefteq G$, χ 是 G 的不可约特征标. 证明存在 H 的不可约特征标 ψ 使 $\chi = \psi^G$ 的充要条件为 χ 在 $G - H$ 上取零值, 并且 $\chi|_H$ 是 H 的若干个彼此不同的不可约特征标的和.

23. 设 χ 是 G 的特征标, 它在 $G - \{1\}$ 上取常数值. 则 $\chi = a1_G + br_G$, 其中 a, b 是整数. 又若 $b > 0$, 则 $\chi(1) \geq |G| - 1$.

24. 设 $|G|$ 是奇数, χ 是 G 的非主不可约特征标, 则 $\chi \neq \overline{\chi}$.

25. 设 $|G|$ 是奇数, $a \in G$, 且对任意的 $\chi \in \mathrm{Irr}(G)$, 恒有 $\chi(a)$ 为实数, 则必有 $a = 1$.

26. 设 $A \leq G$, A 交换，且 $|G:A|$ 是素数方幂. 求证 $G' < G$.

27. 设 χ 是 G 的忠实不可约特征标，且 $\chi(1) = p^a$, p 是素数. 又设 $P \in \mathrm{Syl}_p(G)$, 且 $C_G(P) \nleq P$. 则 $G' < G$.

28. 试造 21 阶非交换群的特征标表.

29. 试造 27 阶非交换群的特征标表.

30. 设 G 是有限交换群，$n = \exp G$. 设 $\mathbf{F}$ 是域，ω 是 $\mathbf{F}$ 上的 n 次本原单位根，则 $\mathbf{F}(\omega)$ 是 G 的分裂域.

31. 设 $\mathbf{F} = GF(p)$ 是 p 个元素的域，$V = V(2, \mathbf{F})$ 是 $\mathbf{F}$ 上二维向量空间. 设 $P \leq GL(V)$, P 是非平凡 p-群. 则 $|P| = p$, 且 V 作为 P-空间是不可分解的，但不是不可约的.

32. 试用矩阵表示的语言来证明 Maschke 定理.

33. 设 X 是 G 的任一复表示，V 是对应的 G-空间. 则可在 V 上规定一个 Hermite 内积，使每个 $X(a)$, $a \in G$, 在 V 上的作用都是 V 的 U-变换.

34. 试用 33 题证明 Maschke 定理 (对基域 $\mathbf{F} = \mathbb{C}$ 的情形.)

35. 设 G 是有限群，$\mathbf{F}$ 是任一域. 则存在 $\mathbf{F}$ 的有限代数扩张 $\mathbf{E}$ 为 G 的分裂域.

36. 证明同构的 A-模有相同的零化子.

37. 证明完全可约模的子模仍为完全可约的.

38. 设 A 是 $\mathbf{F}$-代数，V 是 A-模. 证明 V 是完全可约的当且仅当 V 的所有极大子模的交为 0.

39. 设 A 是 $\mathbf{F}$-代数. 任取一组互不同构的不可约 A-模的完全集 $\{M_1, \cdots, M_s\}$. 令

$$J(A) = \bigcap_{i=1}^{s} \mathrm{Ann}(M_i).$$

证明 $J(A)$ 是有意义的，并且

(1) $J(A)$ 是 A 的双边理想;

(2) 对任一非零 A-模 V, 有 $VJ(A) \subsetneqq V$;

(3) 对某正整数 n 有 $J(A)^n = 0$;

(4) 若 I 是 A 的幂零右理想，即 $I^m = 0$ 对某正整数 m 成立，则 $I \subseteq J(A)$.

我们称 $J(A)$ 为 A 的 Jacobson 根基.

40. 设 A 是 $\mathbf{F}$-代数，证明下列陈述等价:

(1) $J(A) = 0$;

(2) A 中没有非零幂零右理想;

(3) A 中没有非零幂零双边理想;

(4) A 半单.

41. 设 A 是 $\mathbf{F}$-代数，则 $A/J(A)$ 是半单的.

42. 设 V 是 A-模，则 V 是完全可约的当且仅当 $VJ(A)=0$.

附录　研究题

1. 关于群的定义

设 G 是群， I 是非空集合．作积集 $S=G\times I$, 在 S 中定义乘法运算如下：

$$(g,i)(h,j)=(gh,j),\ g,h\in G,\ i,j\in I.$$

证明上述乘法运算是结合的，并且存在一个左单位元，对它来说每个元素皆有右逆．我们称这样的代数系为一个 (l,r) 系．说明它一般不是群．

反过来，设 S 为任一 (l,r) 系，证明 S 有上述之结构，即可找到群 G 和非空集合 I 使 $S\cong G\times I$.

参看文献 [1].

2. 关于群的类数

群 G 的共轭元素类的个数 $k(G)$ 叫做 G 的 类数．E. Landau 解决了 G. Frobenius 提出的一个问题．即他证明了

定理 对于任意的正整数 k, 只有有限多个不同构的有限群 G 使 $k(G)=k$.

证明线索 设 n 阶群 G 有 k 个共轭类，它们包含的元素个数分别为 $h_1=1,h_2,\cdots,h_k$. 对于 $i=1,\cdots,k$, 令 $n_i=n/h_i$, 则 n_i 是正整数．由类方程得

$$\frac{1}{n_1}+\frac{1}{n_2}+\cdots+\frac{1}{n_k}=1. \qquad (*)$$

不妨假定 $n_1 \geq n_2 \geq \cdots \geq n_k$, 则有 $n_k \leq k$. 用对 k 的归纳法可证对任一实数 a, 方程

$$\frac{1}{n_1}+\frac{1}{n_2}+\cdots+\frac{1}{n_k}=a$$

只有有限多组正整数解，从而推出方程 (*) 也有有限多组解. 因 $n_1=n$, 故只有有限多个正整数 n, 使 n 阶群有可能恰含 k 个共轭类. 由此即得定理之结论.

我们以 $n(k)$ 表示具有 k 个共轭类的有限群的阶的最大值，又以 $k(n)$ 表示 n 阶有限群中类数的最小值. 研究下列问题：

(1) 证明 $n(1)=1, n(2)=2, n(3)=6, n(4)=12, n(5)=60$, 等等.

(2) 对于 k 的较小的值，决定类数为 k 的所有有限群.

(3) 给定 n, 寻找 $k(n)$ 的下界，或者等价地，给定 k, 寻找 $n(k)$ 的上界. 对此， Landau 曾证明 $n(k) \leq k^{2^k}$, 参看文献 [2]. 对于幂零群中 $k(n)$ 的估值可参看文献 [3–5].

3. Hamilton 群

我们称非交换群 G 为一个 Hamilton 群，如果 G 的每个子群都是正规子群.

由第 I 章 §3 第 17 题，四元数群 Q_8 是 Hamilton 群. 一般地，我们有下面的

定理　设 Q_8 是四元数群， A 是奇阶交换群， B 是初等交换 2 群. 则 $Q_8 \times A \times B$ 是 Hamilton 群. 反过来，每个有限 Hamilton 群都有上述之形状. 试证明此定理. 可参看 M. Hall 《群论》定理 12.5.4 (中译本第 220 页).

4. 关于次正规子群

关于有限群的次正规子群，最早被 H. Wielandt 所研究. 定理 III,1.9 和 1.10 就是他在文献 [6] 中证明的.

设 G 是有限群，A, B 是 G 的次正规子群，试证明下述结果：

(1) $\langle A, B\rangle$ 的每个合成因子同构于 A 的或 B 的一个合成因子.

(2) 若 $|A:A'|$ 和 $|B:B'|$ 互素，则 $AB=BA$.

(3) 若 $A\cap B=1$, 并且 A,B 没有公共的合成因子是素数阶循环群，则 A,B 间元素可交换 (这推广了第 III 章习题的第 8 题).

(4) 设 S 是 G 的任一次正规子群，则 $N_G(S)$ 包含 G 的任一极小正规子群以及任一本身是非交换单群的次正规子群. 由此得到，若 $G\neq 1$, 则

$$\bigcap_S N_G(S)\neq 1,$$

其中 S 跑遍 G 的所有次正规子群.

为证明上述结果，可参看文献 [6–8]. 为了解有关次正规子群的进一步问题，可参看综述文章 [9].

5. 关于拟正规子群

拟正规子群是正规子群的一种推广.

定义 称 G 的子群 Q 为拟正规子群，如果 Q 与 G 的任一子群 H 可交换，即 $QH=HQ$.

正规子群当然是拟正规子群，但反过来不真. O. Ore 证明了如果 G 的极大子群是拟正规的，则它必为正规子群 (见文献 [10,11]). N. Nakamura 证明了有限群的极小正规子群也一定是极小拟正规子群 (见文献 [15]). 读者试给出这两个结果的各自的证明.

关于拟正规和次正规的关系， O. Ore 在 [12] 中证明了拟正规子群必为次正规的. J. Szép 在 [13] 中改进了上述证明，并把条件进一步减弱. 他证明了，若 $A\leq G$, 且对任意的 $g\in G$ 有 $AA^g=A^gA, \forall g\in G$, 则 $A\lhd\lhd G$.

关于拟正规子群本身的性质， N. Ito 和 J. Szép 在 [14] 中证明了：若 Q 是有限群 G 的拟正规子群，则 Q/Q_G 是幂零群，其中 Q_G 是子群 Q 的核. 换句话说，即无核拟正规子群必为幂零群. W.E. Deskins 曾猜想，无核拟正规子群不仅幂零，而且交换. 但 J.G. Thompson 在 [16] 中举出了一个反例. 他构造了一个 p^{p+5} 阶群，其中 p 为不等于 2 的素数，它包含一个 p^{p+3} 阶非交换的无核拟正规子群. 于是又有两个需进一步研究的问题： (1) 在什么

条件下，有限群的无核拟正规子群是交换的？(2) 对于无核拟正规子群的幂零类和导列长进行估值. 关于这些问题，读者可参看文献 [17–19].

关于拟正规子群，目前还有很多未解决的问题可供进一步研究和探索.

6. 内交换群

在第 III 章 §6 中已经提到，G.A. Miller 和 H.C. Moreno 在 [20] 中决定了所有内交换群的构造，请读者自己定出它们的不同构的类型 (注意，做此问题时应学完前五章). 可参看文献 [21].

7. 可解外交换群和外循环群

尽管 1903 年人们已经弄清了内交换群的构造，但研究外交换群则是在本世纪七十年代的事. 可参看文献 [22,23].

读者试自行证明下面的

定理 1 设 G 是有限可解外交换群.

(1) 若 G 幂零，则 G 为 p- 群，且 $Z(G)$ 循环，$|G'|=p$.

(2) 若 G 非幂零，则 G 有唯一的极小正规子群 N, N 是 p^a 阶的初等交换 p- 群，并且 N 有循环补群 M, 满足

$$M\cap M^g=1,\ \forall g\in G-M.$$

或者换句话说，G 是以初等交换 p- 群为核具有循环补的 Frobenius 群.

反过来，(1) 和 (2) 确系可解外交换群.

至于可解外循环群，我们有下面的

定理 2 设 G 是有限可解外循环群. 则

(1) $G\cong Z_p\times Z_p$;

(2) G 为定理 1 中的 (2) 型群.

试证明此定理.

8. 内幂零群的另一刻画

称有限群 G 为 V- 群，如果 (1) G 有子群 B, 使得 $N_G(B)=C_G(B)$ 是 G 的幂零极大子群，并且 B 的每个真子群为 G 之正规子群； (2) 对任意的 $x\notin N_G(B)$, 有 $\langle B,B^x\rangle=G$.

我们有下面的

定理 *G 是 V- 群等价于 G 是有限内幂零群.*

证明线索 分以下几步：

(1) 证 V- 群必为可解群：分析极小反例.

(2) V- 群定义中的 B 必为素数幂阶循环群.

(3) 证明 B 在 G 中有补 P, P 是 G 的正规 Sylow 子群.

(4) 结合 (1)–(3) 证明 V- 群是内幂零群.

(5) 由内幂零群的结构推知它也是 V- 群.

可参看文献 [24].

9. 关于换位子和换位子群

设 G 是群，则由换位子群的定义有

$$G'=\langle [a,b]\mid a,b\in G\rangle.$$

但一般来说 G' 中的元素并不一定都能表示成 G 中两个元素的换位子. O. Ore 证明，对于对称群 S_n, $n\geq 2$, 恒有 $S_n'=A_n$, 且 A_n 中任一元素均可表成 S_n 中二元素的换位子. 试证明之. 可参看文献 [25].

试举一例说明存在有限群 G 以及 G' 中的某个元素 x, 使得 x 不能表示成 G 中任二元素的换位子. 可参看文献 [26].

10. 关于 Schur-Zassenhaus 定理

Schur-Zassenhaus 定理是有限群论最基本的定理之一. 目前关于正规 Hall 子群的补群的共轭性的证明还需依赖 Feit-Thompson 关于奇数阶群可解性的结果. 很多人企图寻找一个不依赖于这个结果的直接的证明都未获得成功. 但有人不用 Feit-Thompson 定理而改用对 Schreier 猜想正确性的假定，也能证明 Schur-Zassenhaus 定理. 可参看 B. Huppert, “Endliche Gruppen I”, I,18.4. 该证明分两个步骤：

(1) 假定 G 是使 Schur-Zassenhaus 定理中补群共轭性不真的最小阶反例， N 是 G 的正规 Hall 子群，则有

(i) N 和 G/N 都是非交换单群；

(ii) $C_G(N)=1$.

(提示：依下列次序证明： (a) N 是 G 的极小正规子群； (b) $C_G(N)=1$; (c) G/N 是单群； (d) N 是单群.)

(2) 假定 Schreier 猜想的正确性, 证明 Schur-Zassenhaus 定理.

(提示：利用上面 (1) 中的结果.)

11. $GL(3,2)$ 是 168 阶单群

由计算知， $|GL(3,2)|=168$. 试证明 $GL(3,2)$ 为非交换单群，可依下列步骤进行.

设 V 是 $GF(2)$ 上的三维向量空间，则 $GL(3,2)$ 是 V 的全体满秩线性变换组成的群. 于是有

(1) $GL(3,2)$ 可看成 $V^{\#}=V-\{0\}$ 上的置换群 G, 并且 G 是传递的；

(2) $GL(3,2)$ 不是可解群；

(提示：若否，则由第 II 章习题的第 3 题，它的极小正规子群 N 也在 $V^{\#}$ 上传递，必有 $|N|=7$. 于是由 N/C 定理有

$$G/N \lesssim \mathrm{Aut}(Z_7)\cong Z_6.$$

特别地， $|G|\le 42$, 与 $|G|=168$ 矛盾.

(3) $GL(3,2)$ 必为单群.

(提示：利用阶 <168 且为 168 的因子的有限群皆可解.)

更进一步，读者试证明下述事实.

1) $PSL(2,7)$ 是 168 阶单群.

2) 在对称群 S_7 中，由 (1234567) 和 (26), (34) 生成的子群是 168 阶单群.

3) 从同构的意义上来说， 168 阶单群只有一个.

关于 168 阶单群的其它刻划可参看文献 [27–29].

12. 对称群和交错群的自同构群

试证明下述事实:

1) 当 $n \geq 4, n \neq 6$, 有 $\mathrm{Aut}A_n \cong S_n$;

2) 当 $n \geq 3, n \neq 6$, 有 $\mathrm{Aut}S_n \cong S_n$, 因此 S_n 是完全群;

3) $|\mathrm{Aut}A_6| = |\mathrm{Aut}S_6|$, $|\mathrm{Aut}S_6 : \mathrm{Inn}S_6| = 2$.

提示:

(1) 两个不同的也不互逆的 3- 轮换的乘积可能出现下列四种情形 (以不同字母表不同数码):

(i) $(abc)(abd) = (ad)(bc)$,

(ii) $(abc)(adb) = (bcd)$,

(iii) $(abc)(ade) = (abcde)$,

(iv) $(abc)(def)$.

可根据其乘积的阶来确定该二个 3- 轮换属哪种情形.

(2) 为证明 1), 先注意到

$$A_n = \langle (123), (124), \cdots, (12n) \rangle.$$

设 $\theta \in \mathrm{Aut}A_n$. 证明在 $n \geq 4$ 和 $n \neq 6$ 的假设下 θ 把 3- 轮换仍变成 3- 轮换, 进而用 (1) 证明 θ 把 A_n 的上述生成元变为 (abc), $(abd), \cdots, (abl)$, 其中 $a, b, c, d, \cdots, l$ 是 $1, 2, \cdots, n$ 的一个排列, 最后证明 θ 可由 S_n 的一个元素在 A_n 上的共轭作用得到.

(3) 为证明 2), 可利用 I,5.12 的现成结果. 也可由 $S_n = \langle (12), (13), \cdots, (1n) \rangle$ 出发, 分析上述生成元在给定自同构 $\theta \in \mathrm{Aut}S_n$ 之下的像, 仿照 (2) 来导出结论.

(4) 为证明 3), 先证明下面的一般结论: 设 H 是 S_n 的子群, $|S_n : H| = n$. 则存在 $\theta \in \mathrm{Aut}S_n$ 使得 H^θ 为 S_n 的点稳定子群.

然后证明 S_6 中存在指数为 6 的传递子群, 这可由考虑 S_5 在其 Sylow 5- 子群的正规化子上的传递置换表示得到. 于是应用上述一般结论, 可得 $|\mathrm{Aut}S_n| > |\mathrm{Inn}S_n|$.

又因 S_6 中有两个 3 阶元素的共轭类, 每个 S_6 的自同构必互变这两个共轭类或者把它们都变到自身. 于是 $|\mathrm{Aut}S_n : \mathrm{Inn}S_n| \leq 2$.

最后再证明 $|\mathrm{Aut}A_6| = |\mathrm{Aut}S_6|$.

读者可参看文献 [30, Chapter 3, §2].

13. 交换 p- 群的子群个数

试证明关于有限交换 p- 群中给定类型子群个数的下述 Djubjuk 公式 (参看文献 [31]). 为了叙述这个结果, 先引进下面的概念.

首先, 交换 p- 群的 ω- 不变量 $\{\omega_1,\cdots,\omega_e\}$ 由下式规定: $p^{\omega_i} = |\Omega_i(G)/\Omega_{i-1}(G), i=1,2,\cdots,e=e(G)$, 其中 $e(G)$ 是 G 的幂指数, 即满足 $\exp G = p^{e(G)}$; 而 $\Omega_i(G)=\{a\in G \mid a^{p^i}=1\}$. 显然, ω- 不变量满足 $d(G)=\omega_1\geq\omega_2\geq\cdots\geq\omega_e>0$. 为方便起见, 有时也可认为 G 的 ω- 不变量为 $\{\omega_1,\cdots,\omega_e,0,\cdots,0\}$.

设 $\omega_1\geq\omega_2\geq\cdots\geq\omega_e$ 是 e 个非负整数, 而 $\beta_1\geq\cdots\geq\beta_e$ 是任意 e 个整数, 则我们规定数

$$\begin{Bmatrix}\omega_1, & \cdots, & \omega_e\\ \beta_1, & \cdots, & \beta_e\end{Bmatrix} = p^{\sum_{i=1}^{e}(\omega_i-\beta_i)\beta_{i+1}}\prod_{i=1}^{e}\begin{bmatrix}\omega_i-\beta_{i+1}\\ \beta_i-\beta_{i+1}\end{bmatrix}_p, \qquad (*)$$

其中 β_{e+1} 规定为 0, $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}_p$ 的定义见第 I 章例 7.7. 于是我们有

定理 (Djubjuk)设 G 是有限交换 p- 群, 其 ω- 不变量为 $\{\omega_1,\cdots,\omega_e\}$. 又设 $\beta_1,\cdots,\beta_e$ 为任意整数. 则 G 中 ω- 不变量为 $\{\beta_1,\cdots,\beta_e\}$ 的子群个数为

$$\begin{Bmatrix}\omega_1, & \cdots, & \omega_e\\ \beta_1, & \cdots, & \beta_e\end{Bmatrix}.$$

注意, 若 $\beta_1,\cdots,\beta_e$ 不能构成任意交换 p- 群的 ω- 不变量, 则 (*) 式给出的数为 0.

证明可参看文献 [31].

14. 具有 m 阶循环子群的 $4m$ 阶群

试决定所有互不同构的具有 m 阶循环子群的 $4m$ 阶群.

文献 [32] 决定了 m 是奇数的情形.

15. 群阶与群性质的关系

设 $n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$, 其中 $p_1,\cdots,p_s$ 为不同素数, $\alpha_1,\cdots,\alpha_s$ 为正整数. 证明:

(1) n 阶群皆循环的充要条件为 $(n,\varphi(n))=1$;

(2) n 阶群皆交换的充要条件为 (i) 每个 $\alpha_i\le 2$, (ii) 对任意 i,j, 恒有 $(p_j,p_i^{\alpha_i}-1)=1$;

(3) n 阶群皆幂零的充要条件为对任意 i,j, 恒有 $\left(p_i,\prod_{k=1}^{\alpha_j}(p_j^k-1)\right)=1$.

可参看文献 [33].

16. 关于类正规子群和反正规子群

设 G 是有限群, $H\le G$. 称 H 为 G 的*类正规子群*(pronormal subgroup), 如果对任意的 $g\in G$, H 和 H^g 在 $\langle H,H^g\rangle$ 中共轭. 而称 H 为 G 的*反正规子群*(abnormal subgroup), 如果对任意的 $g\in G$ 有 $g\in\langle H,H^g\rangle$.

由上述定义, 正规子群和反正规子群是正相对立的, 但它们却都是类正规子群. 另外, 有限群的 Sylow 子群显然是类正规子群. 读者试证明下述结论:

(1) 设 $K\trianglelefteq G$, 则 K 的每个 Sylow 子群在 G 中类正规;

(2) 设 H 是 G 的类正规子群. 则 $N_G(H)$ 是 G 的反正规子群;

(3) 设 H 是 G 的类正规子群, 同时也是 G 的次正规子群, 则 $H\trianglelefteq G$.

(4) 设 $H\le G$. 则 H 在 G 中反正规的充要条件为对任意的 $K\le G$, $g\in G$, 只要 $H\le K\cap K^g$ 就能推出 $g\in K$;

(5) 设 G 是有限群, p 是素数. 证明每个 p- 子群均在 G 中类正规的充要条件为任一 p- 子群都在包含它的 Sylow p- 子群的正规化子中是正规的.

(提示: (2) 设 $g\notin N=N_G(H)$, 则 $H^g\ne H$. 由 H 的类正规性, 有 $x\in\langle H,H^g\rangle\le\langle N,N^g\rangle$ 使 $H^{gx}=H$, 于是 $gx\in N$. (3) 用 (2). (5) 设 $P\in\mathrm{Syl}_p(G)$, $H\trianglelefteq P$, $H^g\trianglelefteq P$, 则 H 和 H^g 在 $N_G(P)$ 中共轭. 证明并应用这个结论.)

17. 关于特殊子群

称群 G 的子群 H 为**特殊子群**(special subgroup), 如果对任二元素 $x, y \in G$, 其中 $x \notin H$, 都存在唯一的 $h \in H$ 使 $y^{-1}xy = h^{-1}xh$. 试证明:

(1) 若 H 是 G 的特殊子群, $x \in G - H$, 则 $G = C_G(x)H$, 且 $C_G(x) \cap H = 1$;

(2) G 的特殊子群必为正规子群;

(3) 若 H 是 G 的有限阶特殊子群, 则 H 的每个陪集 $Hx(\neq H)$ 组成 G 的一个共轭元素类;

(4) 若 H 是 G 的特殊子群, 则

$$H \supseteq M = \{[x, y] \mid x, y \in G\}.$$

又若 $|H|$ 有限, 则 $H = M$. 特别地, 任一群中至多有一个特殊子群.

(5) 若 H 是 G 的特殊子群, $x \in G - H$, 则子群 $C = C_G(x)$ 是交换群, 并且有

$$C \cap y^{-1}Cy = 1,\ \forall y \in G - C.$$

由此推出 G 是 Frobenius 群.

可参看文献 [34].

18. Frattini 子群的推广

设 G 是有限群. 以 $\Delta(G)$ 表示 G 中所有非正规极大子群的交 (若 G 不存在非正规极大子群, 则命 $\Delta(G) = G$, 显然有 $\Delta(G) \geq \Phi(G)$, 并证明:

(1) $\Delta(G)/\Phi(G) = Z(G/\Phi(G))$;

(2) $\Delta(G)$ 是幂零群;

(3) $\Delta(G)$ 包含 G 的超中心 $Z_\infty(G)$.

可参看文献 [35].

设 G 为有限群. 以 $\Phi_p(G)$ 表示 G 中所有指数与 p 互素的极大子群之交 (若没有这样的极大子群, 则命 $\Phi_p(G) = G$.) 显然有 $\Phi_p(G) \geq \Phi(G)$, 并证明:

(1) 若 $P \in \mathrm{Syl}_p(\Phi_p(G))$, 则 $P \trianglelefteq \Phi_p(G)$, 且 $\Phi_p(G)/P$ 幂零;

(2) 设 p, q 是两个不同的素数, 则

$$\Phi_p(G) \cap \Phi_q(G) = \Phi(G).$$

可参看文献 [36].

19. 有限可补群

称有限群 G 为 **可补群**, 如果对 G 的任一子群 H, 都存在 $K \leq G$ 使 $G = HK$ 且 $H \cap K = 1$. 证明:

(1) 可补群必为可解群;

(2) 可补性在取子群、商群和作直积之下仍然保持;

(3) 若 G 可补, 则 G 的所有主因子循环, 且 G 的所有 Sylow 子群皆为初等交换群;

(4) G 可补的充要条件为 G 是若干个阶无平方因子群的直积的子群.

可参看文献 [37].

20. p^4 阶群 $(p > 3)$

试决定所有互不同构的 p^4 阶群.

(提示: 除掉五种交换群外, 可分四种情形: (i) 亚循环群, 共两种; (ii) 交换正规子群至多为二元生成的非亚循环群, 共三种; (iii) G 有 p^3 阶初等交换子群且 $\exp G = p$, 共两种; (iv) G 有 p^3 阶初等交换子群且 $\exp G = p^2$, 共三种.)

可参看文献 [38] pp. 140–146.

21. 亚循环 2- 群

试决定所有互不同构的亚循环 2- 群. 可参看文献 [39].

并进一步决定导群为循环群的二元生有限 2- 群, 给出一个完全分类 (这至今仍是一个未解决问题).

22. Burnside 问题

W. Burnside 在 1902 年提出一个著名的问题：设 r 是正整数，F_r 是 r 秩自由群. 又设 n 是正整数，$N = \{x^n \mid x \in F_r\}$. 则显然 $N \trianglelefteq F_r$. 命 $B(n,r) = F_r/N$, 问 $B(n,r)$ 是否为有限群？

试证明 $B(2,r)$, $B(3,r)$ 是有限群.

(提示：为证 $B(3,r)$ 有限，可用对 r 的归纳法. 设 $|B(3,k)| = 3^{m(k)}$, 则 $B(3,k+1)$ 可看成 $B(3,k)$ 再添加一个新生成元 z 生成. 于是 $B(3,k+1)$ 中任一元素 g 可表成下列形状：

$$g = u_1 z^{\pm 1} u_2 z^{\pm 1} \cdots z^{\pm 1} u_n,\ u_i \in B(3,k).$$

证明 g 可用最多含两个 z 的上述式子表出.)

对于 Burnside 问题，目前已经证明 $B(2,r)$, $B(3,r)$, $B(4,r)$, $B(6,r)$ 是有限群. 可参看 M. Hall 著《群论》(中译本) 第十八章. 另外 S.I. Adjan 在文献在 [40] 中证明，若 n 是奇数，且 $n \geq 665$, 则 $B(n,r)$ 是无限群.

23. 有限 p- 群的宽

设 G 是有限 p- 群，x 是 G 中任一元素. 若 $|G : C_G(x)| = p^{b(x)}$, 则称 $b(x)$ 为 *元素 x 的宽*(breadth). 又令 $b(G) = \max_{x\in G} b(x)$, 称为 *群 G 的宽*.

J. Wiegold 在 [41] 中有两个猜想：(1) $|G'| \leq p^{\frac{1}{2}b(G)(b(G)+1)}$; (2) $c(G) \leq b(G)+1$. 目前猜想 (1) 已被 M.R. Vaughan-Lee 证明，可见文献 [42]; 而猜想 (2) 已被 V. Felsch 所否定，见文献 [43].

研究下面关于 p- 群的宽的几个简单问题：

1) 证明 $p^{b(G)} \leq |G'|$;

2) 证明 $b(G) = 1$ 的充要条件为 $|G'| = p$.

(提示：设 $b(G) = 1$, 则 (i) $G' \leq Z(G)$, (ii) $\exp G' = p$; (iii) 若 $[a,b] \neq 1 \neq [a',b']$, 则存在 $a'' \in G$ 使 $a'' \notin C_G(b) \cup C_G(b')$. 这时有 $[a'',b] = [a,b]^i$, i 是适当的整数. 可参看文献 [44].)

3) 若 $b(G) < p$, 则 $c(G) \leq b(G)+1$.

(可参看文献 [45].)

24. Lagrange 群

设 G 是有限群, 若对 $|G|$ 的任意正因子 d, G 中都存在 d 阶子群, 则称 G 为 Lagrange 群 (或 CLT- 群). 试证明:

(1) 幂零群是 Lagrange 群;

(2) Lagrange 群是可解群;

(3) 举例说明 Lagrange 群的子群和商群都不一定还是 Lagrange 群;

(4) 设 H 是有限可解群, 则存在有限循环群 K 使 $G = H \times K$ 是 Lagrange 群. 即任一有限可解群都可嵌入一个 Lagrange 群. 进一步还有

(5) 任一有限可解群可嵌入一个 (直积) 不可分解的 Lagrange 群. (可参看文献 [46]).

25. 具有 Sylow 塔之有限群

设 G 是有限群, $|G| = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, 且 $p_1 < \cdots < p_s$. 若存在 G 的正规群列

$$G = G_0 > G_1 > \cdots > G_s = 1 \qquad (*)$$

使得 $|G_{i-1}/G_i| = p_i^{\alpha_i}$, $i = 1, \cdots, s$, 则称群列 (*) 为 G 之一 Sylow 塔, 而称 G 为一具有 Sylow 塔的群, 简称 ST- 群. 试证明下述结果:

(1) ST- 群必为可解群, 但反过来不对;

(2) G 为 ST- 群等价于 $G/\Phi(G)$ 为 ST- 群;

(3) G 为 ST- 群等价于 $G/Z(G)$ 为 ST- 群;

(4) G 为 ST- 群等价于对 G 的每个非平凡子群 H, 都存在 H 的极大子群 K 使得 $|H:K|$ 是 $|H|$ 的最小素因子;

(5) 设群 G 的所有真子群皆为 ST- 群, 则 G 本身必为可解群.

可参看文献 [47].

26. 超可解群

设 G 是有限群. 若 G 的每个主因子皆为循环群, 则称 G 为超可解群. 试证明:

(1) 超可解群必为 ST- 群, 但反过来不对;

(2) 若 G 超可解，则 G' 幂零；

(3) 超可解群的子群、商群和直积仍为超可解群；

(4) 若 G 的每个极大子群皆为超可解群，则 G 本身为可解群；

(5) G 超可解的充要条件为 G 的每个极大子群在 G 中有素数指数.

可参看 M. Hall 的《群论》（中译本）§10.5.

27. 关于可分解群

设有限群 G 可表示成二子群 A, B 的乘积，即 $G = AB$，则称 G 为可分解群. 试证明：

(1) 若 A, B 皆交换，则 G 为亚交换群，即满足 $G'' = 1$；

(提示：因 $A' = B' = 1$，有 $G' = [A, B]$. 对于任意的 $a, a' \in A$, $b, b' \in B$，由 $AB = BA$，可令 $b^{a'} = a''b^*$, $a^{b'} = b''a^*$，其中 $a'', a^* \in A$, $b'', b^* \in B$. 证明 $[a, b]^{a'b'}$ 和 $[a, b]^{b'a'}$ 都等于 $[a^*, b^*]$，于是 $[a, b]$ 和 $[a', b']$ 可交换. 亦可参看文献 [48].)

(2) 设 $G = AB$，则对任意的 $g, g' \in G$，恒有 $G = A^g B^{g'}$，并且存在 $h \in G$ 使 $A^g = A^h$, $B^{g'} = B^h$；

(3) 设 $G = AB$，则存在 $P \in \mathrm{Syl}_p(G)$, $P_1 \in \mathrm{Syl}_p(A)$, $P_2 \in \mathrm{Syl}_p(B)$ 使得 $P = P_1P_2$；更一般地有

(4) 设 $G = AB$，π 是一个素数集合. 如果群 G, A, B 均成立 π-Sylow 定理，即 π-Hall 子群皆存在且共轭，并且任一 π- 子群均属于某一 π-Hall 子群，则必存在 G, A, B 的 π-Hall 子群 H, H_1, H_2 使得 $H = H_1H_2$；

(5) 设 $G = G_1 \cdots G_n$，G_i 是幂零群. 并且对任意的 i, j 有 $G_iG_j = G_jG_i$ 为可解群，则 G 本身可解.

(可参看文献 [49].)

H. Wielandt 在文献 [50] 中证明了下述著名定理：若 $G = AB$, A, B 皆为有限幂零群. 则 G 为可解群.

与此相关的，有下列著名的 Scott 猜想：设 $G = AB$，若 A, B 分别有幂零子群 A_1, B_1 使 $|A : A_1| = 2$, $|B : B_1| = 2$，则 G 是可解群. 这个猜想已在 1979 年被苏联人 Kazarin 证明，可见文献 [51].

28. 极大子群共轭类数 ≤ 2 的有限群

设 G 是有限群. 若 G 的所有极大子群皆共轭, 则必为素数幂阶的循环群 (见 I,7.3). 而若 G 恰有两个极大子群的共轭类, 则 G 必为可解群. 试证明之.

(提示: 以 L, K 表示 G 的两个不共轭的极大子群, 区别以下三种情形: (i) L, K 均为 G 之正规子群, 此时 G 幂零; (ii) L, K 中一个正规, 一个不正规, 证明此时 G 可解; (iii) L, K 皆非 G 之正规子群, 证明这种情形不会发生, 可参看文献 [52].)

注意, 如果 G 恰有三个极大子群的共轭类, 则 G 不一定可解. A_5 和 $PSL(2,7)$ 可作为例子.

进一步还可研究下列问题:

(1) 决定所有恰有两个极大子群共轭类的有限可解群.

(2) 试证明下述结果: 设 G 是恰有三个极大子群共轭类的有限非可解群, 则 $G/\Phi(G)$ 同构于 A_5 或 $PSL(2,7)$.

29. 关于对合中心化子的一个结果

R. Brauer 和 K.A. Fowler 的下述结果在有限单群分类中具有重要的意义 (可参看文献 [53]).

定理 *设 G 是偶阶非交换单群, t 是 G 中任一对合. 令 $m = |C_G(t)|$. 则 $C_G(t) < G$ 且 $|G| \leq (\frac{1}{2}m(m+1))!$.*

这个定理告诉我们, 具有给定的对合中心化子的有限单群只有有限多个. 这个结果可以认为是有限单群分类工作的真正起点.

事实上, 这个结果是下述定理的推论 (请读者自己由下述定理推出上面的结果).

定理 (Brauer-Fowler) *设 G 是偶阶群, 恰有 n 个对合. 又设 $|Z(G)|$ 是奇数. 令 $a = |G|/n$ (a 一般不一定是整数). 则 G 存在子群 H 满足 $|G:H| = 2$ 或 $|G:H| < \frac{1}{2}a(a+1)$.*

(提示: 设 $t_1, \cdots, t_n$ 为 G 中全部对合, 又设 G 中元素共有 k 个共轭类, $1 = x_0, x_1, \cdots, x_{k-1}$ 是诸共轭类的代表元. 再设 c_i 是 G 中满足 $uv = x_i$ 的对合有序偶 (u, v) 的个数, $i = 0, 1, \cdots, k-1$. 则 c_i 是非负整数. 证明:

1) $n^2=\sum_{i=0}^{k-1}c_i|G:C_G(x_i)|$,

2) 若 x_i 不是对合, $x_i\neq 1$, 则 c_i 是满足 $x_i^t=x_i^{-1}$ 的对合 t 的个数；若 x_i 是对合，则 c_i+1 是 $C_G(x_i)$ 中的中的对合数；又，$c_0=n$.

3) 设 $x\in G$, 命

$$C_G^*(x)=\{g\in G\mid x^g=x\text{ 或}x^{-1}\},$$

并称之为 x 在 G 中的广义中心化子. 则 $C_G^*(x)\leq G$, 且若 $x^2=1$ 或 x 是 G 中非实元素(称 x 为 G 中的实元素, 如果 x 和 x^{-1} 共轭), 则 $C_G^*(x)=C_G(x)$; 而若 $x^2\neq 1$ 且 x 为实元素, 则 $|C_G^*(x):C_G(x)|=2$.

4) 设 $x\in G$, 若 x 是 G 中实元素，则满足 $x^g=x^{-1}$ 的元素 $g\in G$ 的个数等于 $|C_G(x)|$.

5) 对每个 $i=0,1,\cdots,k-1$, 有 $c_i\leq|C_G(x_i)|$. 并且若 x_i 不是实元素，则 $c_i=0$; 而若 x_i 是对合，则 $c_i\leq|C_G(x_i)|-2$.

6) 定理的证明：设 $x_0,x_1,\cdots,x_{k-1}$ 如此编号使 $x_1,\cdots,x_s$ 是对合，$x_{s+1},\cdots,x_{r-1}$ 是实元素但非对合，而 $x_r,\cdots,x_{k-1}$ 是非实元素，并有 $0<s\leq r-1\leq k-1$. 因每个对合共轭于 $x_1,\cdots,x_s$ 中的一个，故有

$$n=\sum_{i=1}^{s}|G:C_G(x_i)|. \tag{1}$$

由上式及 1), 2), 5) 可得

$$\begin{aligned}n^2 \leq\ & n+\sum_{i=1}^{s}(|C_G(x_i)|-2)|G:C_G(x_i)|\\ &+\sum_{i=s+1}^{r-1}|C_G(x_i)||G:C_G(x_i)|,\end{aligned}$$

并由计算得到

$$n^2\leq(r-1)|G|-n. \tag{2}$$

设 $j=\min\{|G:H|\mid H<G\}$. 若 $j=2$, 定理结论成立，故可设 $j>2$. 因 $|Z(G)|$ 是奇数，故 $Z(G)$ 中无对合，于是 $C_G(x_i)<G;i=$

$1, \cdots, s$. 从而 $j \le |G : C_G(x_i)|$, $i = 1, \cdots, s$. 由 (1) 式有

$$sj \le n. \tag{3}$$

对 $i = s+1, \cdots, r-1$, 由 3) 可得 $|C_G^*(x_i) : C_G(x_i)| = 2$. 因 $j > 2$, 有 $C_G^*(x_i) < G$. 于是 $j \le |G : C_G^*(x_i)|$, 即

$$j \le \frac{1}{2}|G : C_G(x_i)|, \text{ 对} i = s+1, \cdots, r-1. \tag{4}$$

计算实元素总数，可推得

$$1 + n + 2j(r - s - 1) \le |G|. \tag{5}$$

由 (2) 式得

$$\begin{aligned} n^2 &\le s|G| + (r-s-1)|G| - n \\ &\le \frac{n|G|}{j} + \frac{(|G|-1-n)|G|}{2j} - n. \end{aligned}$$

再用 (3), (5) 二式推出

$$n^2 \le \frac{n|G|}{2j} + \frac{|G|^2}{2j} - \frac{|G|}{2j} - n.$$

注意到 $|G|/n = a$, 由上式即可推出 $j < \frac{1}{2}a(a+1)$.

30. 有限群的 Cayley 图

设 G 是有限群, S 是 G 的一个生成系，且 $1 \notin S$. 我们构造一个有向图 $X = X(G, S)$ (关于图的概念可参看任何一本图论教科书，这里不作说明), X 的顶点集合 $V(X) = G$, 而边集合 $E(X) = \{(g, h) \mid g, h \in G, \text{且} hg^{-1} \in S$, 叫做群 G 关于生成系 S 的 Cayley有向图(Cayley digraph).

若对 S 中的每一元素 s_i, 指定一种颜色 c_i 与之对应. 并对 Cayley 有向图 X 的边如下着色：若 $(g, h) \in E(X)$ 且 $hg^{-1} = s_i$, 则把边 (g, h) 着 c_i 色，这样得到的边着色图叫做 G 关于 S 的 Cayley色图(Cayley colored graph).

又若 S 满足条件 $S^{-1}=S$, 则 X 的边集合 $E(X)$ 满足: $(g,h)\in E(X)$ 当且仅当 $(h,g)\in E(X)$. 于是可以无向边 gh 代替这两个边 (g,h) 和 (h,g). 这时得到的图是无向图, 叫做 G 关于 S 的 Cayley图(Cayley graph).

称 G (作为集合) 的一个置换 α 为 Cayley 有向图或无向图 $X=X(G,S)$ 的一个自同构, 如果 $(g,h)\in E(X)$ 当且仅当 $(g^\alpha,h^\alpha)\in E(X)$. 对于 Cayley 色图而言, 称 G 的置换 α 为 X 的一个保色自同构, 如果 α 是 X 的自同构, 并且对任意的边 $(g,h)\in E(X)$, (g,h) 和 (g^α,h^α) 着色相同. 试证明以下结论:

(1) 有限群的 Cayley 图是连通的, 而 Cayley 有向图是强连通的;

(2) G 关于任一生成系 S 的 Cayley 色图的全体保色自同构组成一个群 $\mathrm{Aut}_c(X)$, 且它同构于 G 的右乘变换群 $R(G)$. 特别地, $\mathrm{Aut}_c(X)$ 在 G 上的作用是传递的;

(3) Cayley 有向图 (或 Cayley 图) X 的自同构群 $\mathrm{Aut}(X)\geq \mathrm{Aut}_c(X)$, 并举出使 $\mathrm{Aut}(X)\neq \mathrm{Aut}_c(X)$ 的例子;

(4) 设 X 是顶点传递的连通有向图 (无向图), 即 $\mathrm{Aut}(X)$ 在 $V(X)$ 上的作用是传递的. 则 X 是某个群 G 关于生成系 S 的 Cayley 有向图 (或 Cayley 图) 的充要条件是 $\mathrm{Aut}(X)$ 存在正则子群.

(5) 试找一个顶点传递有向图或无向图, 它不是任一群的 Cayley 有向图或 Cayley 图.

(提示: 著名的 Petersen 图可作为一例, 试证明之.)

研究题参考文献

[1] Mann, H.B., On certain systems which are almost groups, *Bull. Amer. Math. Soc.*, **50**(1944), 879–881.

[2] Brauer, R., Representations of finite groups, in *Lectures on Modern Mathematics*, vol. 1, New York, Wiley, 1963. pp. 133–175.

[3] Ayoub, C.W., On the number of conjugate classes in a group, in *Proc. Internat. Conf. Theory of Groups*, Austral. Nat. Univ., Canberra, 1965, Gordon & Breach Science Publishers, Inc., 1967. pp. 7–10.

[4] Sherman, G., A lower bound for the number of conjugacy classes in a finite nilponent group, *Pacific J. Math.*, **80**(1979), 253–254.

[5] Poland, J., Two problems on finite groups with k conjugacy classes, *J. Austral. Math. Soc.*, **8**(1968), 45–55.

[6] Wielandt, H., Eine Verallgemeinerung der invarianten Untergruppen, *Math. Z.*, **45**(1939), 209–244.

[7] Wielandt, H., Vertauschbare nachinvariante Untergruppen, *Abh. Math. Sem. Univ. Hamburg*, **21**(1957), 55–62.

[8] Wielandt, H., Über den Normalisator subnormaler Untergruppen, *Math. Z.*, **69**(1958), 463–465.

[9] Wielandt, H., On the structure of composite groups, in *Proc. Internat. Conf. Theory of Groups*, Austral. Nat. Univ., Canberra, 1965, Gordon & Breach Science Publishers, Inc., 1967. pp. 379–388.

[10] Ore, O., Structures and group theory I, *Duke Math. J.*, **3**(1937), 149–174.

[11] Ore, O., A remark on the normal decompositions of groups, *Duke Math. J.*, **5**(1939), 172–173.

[12] Ore, O., Contributions to the theory of groups, *Duke Math. J.*, **5**(1939), 431–460.

[13] Szép, J., Bemerkung zu einem Satz von O. Ore, *Publ. Math. Debrecen*, **3**(1953), 81–82.

[14] Ito, N. and Szép, J., Über die Quasinormalteiler von endlichen Gruppen, *Acta Sci. Math. (Szeged)*, **23**(1962), 168–170.

[15] Nakamura, K., Beziehungen zwischen den Normalteiler und Quasinormalteiler, *Osaka J. Math.*, **7**(1970), 321–322.

[16] Thompson, J.G., An example of core-free quasinormal subgroup of p-groups, *Math. Z.*, **96**(1967), 226–227.

[17] Bradway, R.H., Gross, F. and Scott, W.R., The nilponence class of core-free quasinormal subgroups, *Rocky Mountain J. Math.*, **1**(1971), 541–550.

18] Gross, F., p-subgroups of core-free quasinormal subgroups, *Rocky Mountain J. Math.*, **1**(1971), 375–382.

[19] Nakamura, K., Characteristische Untergruppen von Quasinormalteilern, *Arch. Math.*, **32**(1979), 513–515.

[20] Miller, G.A. and Moreno, H.C., Non-abelian groups in which every subgroup is abelian, *Trans. Amer. Math. Soc.*, **4**(1903), 398–404.

[21] 陈重穆, 内 Σ- 群, 数学学报, **23**(1980), 239–243; **24**(1981), 331–335.

[22] Klein, T., Groups whose proper factors are all abelian, *Isreal J. Math.*, **9**(1971), 362–366.

[23] Baartmans, A.H., Groups whose proper factors are abelian, *Acta Math. Acad. Sci. Hungar.*, **27**(1976), 33–36.

[24] Niemermaa, M., A characterization of minimal nonnilpotent groups, *Arch. Math.*, **38**(1982), 385–387.

[25] Ore, O., Some remarks on commutators, *Proc. Amer. Math. Soc.*, **2**(1951), 307–314.

[26] Cassidy, P.J., Products of commutators are not always commutators: an example, *Amer. Math. Monthly*, **96**(1979), 772.

[27] Adnan, S., A characterization of $PSL(2,7)$, *J. London Math. Soc.*, (2)**17**(1976), 215–225.

[28] Adnan, S., A further characterization of projective special linear group, *J. Austral. Math. Soc. Ser. A*, **24**(1977), 112–116.

[29] 施武杰 (Shi Wujie), A characteristic property of $PSL_2(7)$, *J. Austral. Math. Soc. Ser. A*, **36**(1984), 354–356.

[30] Suzuki, M., *Group Theory I*, Springer-Verlag, 1982.

[31] Djubjuk, P.E., On the number of subgroups of finite abeliaan groups (Russian), *Dokl. Akad. Nauk SSSR*, **137**(1961), 506–508.

[32] 白述伟，具有奇数 m 阶循环子群的 $4m$ 阶有限群之完全分类，**哈尔滨师范大学学报 (自然科学版)**, 1983 年，第 2 期， 22–30.

[33] 张远达，有限群构造 (下册), 第八章 §6, 科学出版社， 1982.

[34] Schwerdtfeger, H., Über eine spezille Klasse Frobeniusscher Gruppen, *Arch. Math.*, **13**(1962), 283–289.

[35] Gaschütz, W., Über die Φ-Untergruppe endlicher Gruppen, *Math. Z.*, **58**(1953), 160–170.

[36] Deskins, W.E., On maximal subgroups, in *Proc. Symp. Pure Math.* vol. 1, pp. 100–104.

[37] Hall, P., Complemented groups, *J. London Math. Soc.*, **12**(1937), 201–204.

[38] Burnside, W., *Theory of Groups of Finite Order*, 2nd ed., New York, Dover, 1955.

[39] King, B.W., Presentations of metacyclic groups, *Bull. Aus. Math. Soc.*, **8**(1973), 101–131.

[40] Adjan, S.I., *The Burnside Problem and Identities in Groups* (Russian), 1975. An English translation (translated by J. Lennox & J. Wiegold) was published by Springer-Verlag, Berlin, 1979.

[41] Wiegold, J., Groups with boundedly finite classes of conjugate elements, *Proc. Roy. Soc. Ser. A*, **238**(1957), 389–401.

[42] Vaughan-Lee, M.R., Breadth and commutator subgroups of p-groups, *J. Algebra*, **32**(1976), 278–285.

[43] Felsch, V., The computation of a counterexample to the class-breadth conjecture for p-groups, *Proc. Symp. Pure Math.*, **37**(1980), (Santa Cruz, 1979), 503–506.

[44] Knoche, H.G., Über den Frobeniusschen Klassenbegrift in nilpotenten Gruppen, *Math. Z.*, **55**(1951), 71–83.

[45] Leedham-Green, C., Neumann, P.M. and Wiegold, J., The breadth and the class of a finite p-group, *J. London Math. Soc.*, **1**(1969), 409–420.

[46] Gagen, T.M., A note on groups with the inverse Lagrange property, in *Group Theory: Proc. of Miniconf.* held at Austral. Nat. Univ., Canberra, 1975, Lecture Notes in Math. 573, Springer-Verlag, 1977. pp. 51–52.

[47] Hawkes, T., On the class of Sylow tower groups, *Math. Z.*, **105**(1968), 393–398.

[48] Ito, N., Über das Produkt von zwei abelschen Gruppen, *Math. Z.*, **62**(1955), 400–401.

[49] Wielandt, H., Über das Produkt von paarweise vertauschbaren nilpotenten Gruppen, *Math. Z.*, **55**(1951), 1–7.

[50] Wielandt, H., Über Produkte von nilpotenten Gruppen, *Illnois J. Math.*, **2**(1958), 611–618.

[51] Kazarin, L.S., On products of two groups, which are almost nilpotent (Russian), *Mat. Sb.*, **110 (152)**(1979), 51–65.

[52] 徐明曜 (Xu Mingyao), Another proof of the solvability of finite groups with at most two conjugacy classes of maximal subgroups, *Chin. Ann. Math.* **6B**(1985), 211–213.

[53] Brauer, R. and Fowler, K.A., On groups of even order, *Ann. of Math.*, (2)**62**(1955), 565–583.

[54] Biggs, N., *Algebraic Graph Theory*, Cambr. Univ. Press, 1974. Chapter 16.

上册习题提示

第 I 章

§1.

5. 取 g_1, g_2 为 g 的适当方幂.

7. 设有两个 q 阶子群 Q_1, Q_2. 用定理 1.18 计算 $|Q_1Q_2|$, 从而推出矛盾.

10. **解法一**: 只须处理 $H \neq H^x$ 的情形. 因为 H 只有两个共轭子群, 故它们就是 H 和 H^x. 我们要证明 $\langle H, H^x\rangle = HH^x$. 因为 $\langle H, H^x\rangle$ 中元素总可表示成 $h_1h_2^xh_3h_4^x\cdots$ 的形状, 其中 $h_i \in H$. 利用

$$h_1h_2^xh_3 = h_2^{xh_1^{-1}}(h_1h_3),$$

而 $h_2^xh_1^{-1}$ 或 $\in H$, 或 $\in H^x$, 故仍可写成 h 或 h^x 的形状, 这就可使上述有限积的长度缩短. 继续作下去, 即可把它化成 hh'^x 的形状.

解法二: 应用 §2 中正规子群的概念. 由 $N_G(H) \trianglelefteq G$, 而 $H \trianglelefteq N_G(H)$, $H^x \trianglelefteq N_G(H)$, 立得结论.

11. 设 $\langle H_1, \cdots, H_n\rangle$ 中一般元素的形状为

$$a_1a_2\cdots a_s, a_j \in H_{i_j}, j = 1, 2, \cdots, s.$$

利用 $xy = y^{x^{-1}}x$ 设法把上述表达式中的长度 s 缩短, 或者把脚标集 $i_1, i_2, \cdots, i_s$ 排成由小到大的次序.

12. 考虑元素 $a_1, a_1a_2, a_1a_2a_3, \cdots, a_1a_2\cdots a_n$. 如果它们都不为 1, 则必有二元素相等.

13. 若 $a_ia_j = a_k \in K$, 则 ${a_i}^{-1}a_k = a_j$, 反之亦然. 因此属于 K 的形如 a_ia_j 的乘积个数等于属于 K 的形如 ${a_i}^{-1}a_k$ 的乘积个数. 因为 $1 \notin K^2$, 故有 $1 \notin K$ 且 $K^{-1} \cap K = \varnothing$. 于是 ${a_i}^{-1}a_i = 1 \notin K$, 且若 ${a_i}^{-1}a_k \in K$, 则其逆 ${a_k}^{-1}a_i \notin K$. 由此推出所需之结论.

16. 利用 15 题，有

$$A = A(A\cap C) = A(B\cap C) = B\cap AC = B\cap BC = B.$$

18. 本题中三问都不成立.

§2.

6. 设 H 是群，满足 $Z(H)=1$. 假定 $1\neq a\in H, o(a)=n$. 令 $K=\langle b\rangle$ 是 n 阶循环群，作直积 $G=H\times K$. 显然有 $Z(G)=Z(H)\times Z(K)=K$. 这时映射

$$\alpha: hb^i\mapsto a^i,\ h\in H, i=0,1,\cdots,n-1$$

是 G 的自同态，但 $K^\alpha=\langle a\rangle\not\subseteq K$.

9. 由 Aut(G)=1 得 Inn(G)=1. 据第 7 题， $G=Z(G)$, 即 G 是交换群. 于是映射 $g\mapsto g^{-1},\forall g\in G$ 是 G 的自同构. 由 Aut(G)=1 推知 $g=g^{-1},\forall g\in G$, 即 $\exp G\leq 2$. 把 G 看成 $GF(2)$ 上的向量空间的加法群(运算看作加法), 证明若该空间的维数 ≥ 2, 则 G 有非恒等的自同构.

13. 由 $N_G(S)=G$ 知 S 为 G 的若干个共轭元素类 $C_1,\cdots,C_k$ 的并. 于是有

$$\langle S\rangle=\langle C_1\rangle\cdots\langle C_k\rangle,$$

因此，不失普遍性可假设 $k=1$, 即 $S=\{s_1,\cdots,s_m\}$ 是 G 的一个共轭元素类，据 §1 第 11 题，

$$\langle S\rangle=\langle s_1\rangle\cdots\langle s_m\rangle,$$

由此立得所需之结论.

14. 设 $N=N_G(H)$, 则 $H\trianglelefteq N$ 且 $|N:H|$ 是 $|G:H|=n$ 的因子. 作商群 N/H, 有 $|N/H|\mid n$. 因为 $z\in Z(G)$, 自然有 $z\in N$, 于是 $z^n\in H$.

15. 首先，诸 S_i 中至少有一个包含群的单位元素 1, 不妨设 $1\in S_1$. 于是对任意的 i 有

$$S_i=\{1\}S_i\subseteq S_1S_i\subseteq S_k,\ \text{对某个 } k \text{ 成立}.$$

据条件 (2) 得 $S_k=S_i$, 于是 $S_1S_i=S_i$. 同理可证 $S_iS_1=S_i$. 特别地，有 $S_1S_1=S_1$. 下面依次证明:

1) 对于 $i\neq 1$, 有 $1\notin S_i$. 即诸 S_i 中只有一个，即 S_1 包含单位元素 1;

2) ${S_1}^{-1}=S_1$ 从而 S_1 是 G 的子群;

3) 每个 S_i 都是 S_1 的右陪集: 首先证 S_i 是 S_1 的若干个右陪集的并，再证 S_i 只能是 S_1 的一个右陪集;

4) 每个 S_i 也是 S_1 的左陪集，从而 S_1 是 G 的正规子群.

§3.

2. 若 $p \neq 2$, 由初等数论, p^n 存在原根; 而当 $p=2, n>2$, 虽 2^n 不存在原根, 但模 2^n 的简化剩余系可以 $\pm 5^i, i=1,2,\cdots,2^{n-2}$ 作为其代表元.

9. 设 α 的轮换分解式为

$$\alpha=(a_{11}^{(1)}\cdots a_{1l_1}^{(1)})\cdots(a_{n_11}^{(1)}\cdots a_{n_1l_1}^{(1)})\cdot$$
$$(a_{11}^{(2)}\cdots a_{1l_2}^{(2)})\cdots(a_{n_21}^{(2)}\cdots a_{n_2l_2}^{(2)})\cdot$$
$$\cdots\cdot(a_{11}^{(s)}\cdots a_{1l_s}^{(s)})\cdots(a_{n_s1}^{(s)}\cdots a_{n_sl_s}^{(s)}).$$

如果 $\beta \in C_{S_n}(\alpha)$, 则

$$\alpha=\beta^{-1}\alpha\beta=(a_{11}^{(1)\beta}\cdots a_{1l_1}^{(1)\beta})\cdots(a_{n_11}^{(1)\beta}\cdots a_{n_1l_1}^{(1)\beta})\cdot$$
$$(a_{11}^{(2)\beta}\cdots a_{1l_2}^{(2)\beta})\cdots(a_{n_21}^{(2)\beta}\cdots a_{n_2l_2}^{(2)\beta})\cdot$$
$$\cdots\cdot(a_{11}^{(s)\beta}\cdots a_{1l_s}^{(s)\beta})\cdots(a_{n_s1}^{(s)\beta}\cdots a_{n_sl_s}^{(s)\beta}).$$

因为每一 k 轮换有 k 种不同写法, 又等长的轮换可以调换位置, 故满足 $\beta^{-1}\alpha\beta=\alpha$ 的 β 的选法应该有 $n_1!l_1{}^{n_1}n_2!l_2{}^{n_2}\cdots n_s!l_s{}^{n_s}$ 种, 此即为 $C_{S_n}(\alpha)$ 的阶. 由此又得 α 所在的共轭类的长为 $\frac{n!}{n_1!l_1{}^{n_1}n_2!l_2{}^{n_2}\cdots n_s!l_s{}^{n_s}}$.

10. α 在 S_n 中的共轭类也是在 A_n 中的共轭类的充分必要条件为

$$\frac{|S_n|}{|C_{S_n}(\alpha)|}=\frac{|A_n|}{|C_{A_n}(\alpha)|}=\frac{|S_n|}{2|C_{S_n}(\alpha)\cap A_n|},$$

即 $|C_{S_n}(\alpha)|=2|C_{S_n}(\alpha)\cap A_n|$. 注意到 $|S_n:A_n|=2$, 上述条件等价于 $C_{S_n}(\alpha)\not\subseteq A_n$.

若 $C_{S_n}(\alpha)\subseteq A_n$, 由计算可得 α 在 A_n 中的共轭类长度为它在 S_n 中共轭类长度的一半, 故此时分裂为两个长度相等的共轭类.

最后, 若 α 的轮换分解式中诸轮换长度皆为奇数且互不相等, 譬如设

$$\alpha=(a_1^{(1)}\cdots a_{l_1}^{(1)})(a_1^{(2)}\cdots a_{l_2}^{(2)})\cdots(a_1^{(s)}\cdots a_{l_s}^{(s)}),$$

其中 $l_1,\cdots,l_s$ 为互不相等之奇数. 如果 $\beta\in C_{S_n}(\alpha)$, 即满足 $\beta^{-1}\alpha\beta=\alpha$, 则易推出

$$\beta=(a_1^{(1)}\cdots a_{l_1}^{(1)})^{i_1}(a_1^{(2)}\cdots a_{l_2}^{(2)})^{i_2}\cdots(a_1^{(s)}\cdots a_{l_s}^{(s)})^{i_s},$$

其中 $i_1,\cdots,i_s$ 为适当的整数. 因此 β 为偶置换, 即 $\beta\in A_n$. 反之, 若 α 的轮换分解式不是上述形状, 则存在奇置换 $\beta\in C_{S_n}(\alpha)$.

11. 用命题 3.15 及第 10 题的结论.

12. 算出 A_5, A_6 诸共轭类的长度，并注意到正规子群是若干个共轭类的并.

13. 令 $\alpha = (12\cdots n)$, 则 $C_{S_n}(\alpha) = C_{S_n}(\langle\alpha\rangle)$. 若 $\beta \in C_{S_n}(\alpha)$, 即 $\beta^{-1}\alpha\beta = \alpha$, 于是有

$$(1^\beta 2^\beta \cdots n^\beta) = (12\cdots n).$$

这样，对某正整数 $i, 1 \le i \le n$, 有

$$\begin{aligned}\beta &= \begin{pmatrix} 1 & 2 & \cdots & n-i+1 & n-i+2 & \cdots & n \\ i & i+1 & \cdots & n & 1 & \cdots & i-1 \end{pmatrix} \\ &= (12\cdots n)^i \in \langle\alpha\rangle.\end{aligned}$$

14. 设有限群 G 只有唯一的极大子群 M, 则任取 $a \notin M$, 则必有 $G = \langle a \rangle$, 于是 G 是循环群.

19. 设 $D_{2^{n+1}} = \langle a, b \rangle$, 有定义关系:

$$a^{2^n} = b^2 = 1, b^{-1}ab = a^{-1}.$$

又设 $N \trianglelefteq D_{2^{n+1}}$, N 非循环, 则有 $ba^i \in N$, 对某个整数 i. 由 N 的正规性, $(ba^i)^a \in N$. 但

$$(ba^i)^a = a^{-1}ba^{i+1} = b(b^{-1}a^{-1}b)a^{i+1} = ba^{i+2},$$

于是 $a^2 = (ba^i)^{-1}(ba^{i+2}) \in N$. 这样 $N = \langle a^2, b \rangle$, 或者 $N = \langle a^2, ba \rangle$.

20. 设 $G = \langle x, y \rangle$, x, y 是两个 2 阶元. 令 $a = xy$, 于是 $\langle a \rangle \trianglelefteq G$, 且 $G = \langle a, x \rangle$, 有二面体群之定义关系.

§4.

2. 利用 §1 第 4 题或本节第 1 题.

4. 利用第 1 题.

6. 分别 p^2 阶循环群和初等交换 p 群两种情形计算之: p^2 阶循环群个数为

$$\frac{p^4 - p^2}{p^2 - p} = p^2 + p,$$

而 p^2 阶初等交换 p 子群只有一个，故共有 $p^2 + p + 1$ 个.

8. 利用交换群分解定理，任一非循环之交换群必含有 p^2 阶初等交换 p 群 (对某个素数 p). 再根据域中方程 $x^p = 1$ 至多有 p 个解推出所需之结论.

10. 用对 n 的归纳法.

§5.

1. 可令 $D_8=\langle a,b\rangle$, 有定义关系：

$$a^4=b^2=1, b^{-1}ab=a^{-1}.$$

若 $\alpha\in\mathrm{Aut}(D_8)$, 则 a^α, b^α 亦为 D_8 之生成元并满足同样的定义关系. 由此分析 a^α, b^α 的各种可能性.

2. 应用和第 1 题相同的方法.

4. 考虑 $GF(3)$ 上的三阶对角阵

$$A=\begin{pmatrix}-1&&\\&1&\\&&1\end{pmatrix}, B=\begin{pmatrix}1&&\\&-1&\\&&1\end{pmatrix}, C=\begin{pmatrix}1&&\\&1&\\&&-1\end{pmatrix}.$$

令 $H=\langle A,B,C\rangle$, 则 H 是 $GL(3,3)$ 中的子群，它同构于 8 阶初等交换 2 群.

再令

$$D=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}.$$

由计算可得 $D^{-1}AD=B, D^{-1}BD=C, D^{-1}CD=A$. 最后令 $G=\langle H,D\rangle$, 则有 $H\trianglelefteq G$. 这时 $|\mathrm{Aut}(H)|=168$, 而用和第 1 题相同的方法易证明 $|\mathrm{Aut}(G)|\le 56$.

6. 取 $M=C_G(N)$.

8. 对任意的 $g\in G, gg^\alpha\in G_1, g(g^{-1})^\alpha\in G_2$. 再用条件 $(2,|G|)=1$.

9. 这时 G_1 仍为 G 之子群，但 G_2 不一定. 对于任意的 $g\in G$, 有 $(g^{-1}g^\alpha)^i\in G_2$, 其中 i 为任意整数. 由 $(2,|G|)=1$, 存在正整数 k 使 $(g^{-1}g^\alpha)^{2k}=g^{-1}g^\alpha$. 令 $y=(g^{-1}g^\alpha)^k$, 易验证 $(gy)^\alpha=gy$, 即 $gy\in G_1$. 于是 $g=(gy)y^{-1}\in G_1G_2$.

10. 由条件，对任意的 $g\in G$, 可设 $g^\alpha=h(g)\cdot g$, 其中 $h(g)\in H$. 我们要证 $h(g)\in H^x, \forall x\in G$. 因为 α 是自同构，有 $(xg)^\alpha=x^\alpha g^\alpha$. 由此得

$$h(xg)xg=h(x)xh(g)g,$$

这推出 $xh(g)x^{-1}=(h(x))^{-1}h(xg)\in H$, 故 $h(g)\in H^x$.

11. 前一结论由直接验证可得. 为证后一结论，我们设由 x 诱导出的 G 的内自同构 $\sigma(x)$ 是中心自同构，则易证 x 满足

$$g^{-1}x^{-1}gx\in Z(G), \forall g\in G.$$

这说明 $xZ(G)\in Z(G/Z(G))$. 最后验证映射 $\sigma(x)\mapsto xZ(G)$ 即为中心内自同构群到 $Z(G/Z(G))$ 上的同构.

12. 由 $x^{-1}x^{\alpha}=y^{-1}y^{\alpha}$ 推出 $yx^{-1}=(yx^{-1})^{\alpha}$. 因 α 是无不动点自同构, 得 $yx^{-1}=1$, 即 $y=x$. 这说明映射 $x\mapsto x^{-1}x^{\alpha}$ 是 G 到自身的单射. 由 G 的有限性, 它也必为满射. 即 $G=\{x^{-1}x^{\alpha}\big|x\in G\}$.

13. 对任意的 $g\in G$, 有

$$(g^{-1}g^{\alpha})^{\alpha}=(g^{\alpha})^{-1}g=(g^{-1}g^{\alpha})^{-1}.$$

由 12 题, 即得对任意的 $x\in G$ 有 $x^{\alpha}=x^{-1}$. 再据第 7 题, G 是交换群. 最后由 α 是无不动点的推出 $|G|$ 是奇数.

14. 用 N/C 定理, $G/C_G(N)\lesssim \mathrm{Aut}(N)$. 由 N 循环, 得 $\mathrm{Aut}(N)$ 交换, 故 $C_G(N)\geq G'$.

§6.

1. 应用例 6.6 的结论, 或模仿例 6.6 的方法.

2. 利用 $(ab)^3=1$ 推出 $bab=a^{-1}ba^{-1}, ba^{-1}b=aba$. 再由此二式推出 $a(ba^2b)=(ba^2b)a^{-1}$. 由这些关系可推出 G 的任一元素均可表成 a^i, a^iba^j, a^iba^2b 之形状, 其中 i,j=0,1,2,3. 因此 $|G|\leq 4+4\times4+4=24$. 又, 在 S_4 中令 $a=(1234), b=(12)$, 则 $ab=(234)$, 有关系 $a^4=b^2=(ab)^3=1$. 于是 S_4 是 G 的同态像. 因 $|S_4|=24$, 这就迫使 $G\cong S_4$.

3. 由定义关系组可推出以下诸式:

$$\begin{aligned}&bab=a^{-1}ba^{-1}, ba^{-1}b=aba,\\&ba^2b=a^{-1}(ba^{-2}b)a^{-1}, ba^{-2}b=a(ba^2b)a,\\&ba^2ba^2b=a^{-1}(ba^2b)a^{-1}, ba^{-2}ba^{-2}b=a(ba^{-2}b)a,\\&ba^{-2}ba^2b=a(ba^2ba^{-2}b)=(ba^2ba^{-2}b)a^{-1}.\end{aligned}$$

应用上面关系推出 G 中元素均可表成

$$a^i, a^iba^j, a^i(ba^2b)a^j, a^i(ba^2ba^{-2}b)$$

之形状, 其中 $i,j=0,1,2,3,4$. 于是有 $|G|\leq 60$. 又在 A_5 中令 $a=(12345), b=(12)(34)$, 则 $ab=(245)$, 满足关系 $a^5=b^2=(ab)^3=1$, 于是 A_5 是 G 的同态像. 再由 $|A_5|=60, |G|\leq 60$, 就迫使 $G\cong A_5$.

4. 先证明 $|G|\leq n!$. 用对 n 的归纳法. 令 $H=\langle a_1,a_2,\cdots,a_{n-2}\rangle$. 由归纳假设, $|H|\leq(n-1)!$. 于是只须证 $|G:H|\leq n$. 考虑 H 的 n 个右陪集 $H, Ha_{n-1}, Ha_{n-1}a_{n-2},\cdots,Ha_{n-1}a_{n-2}\cdots a_1$. 设法证明用任意的 a_j 右

乘这些陪集得到它们的一个置换．（注意，我们并不需要证明上述 n 个陪集两两不同．）

再在 S_n 中令 $\pi_i = (i\ i+1), i = 1, 2, \cdots, n-1$. 验证 $\pi_1, \pi_2, \cdots, \pi_{n-1}$ 满足与 $a_1, a_2, \cdots, a_{n-1}$ 同样的关系．于是 S_n 是 G 的同态像．由 $|S_n| = n!$ 得 $G \cong S_n$.

5. 设 $G = \langle a_1, \cdots, a_r \rangle$. 令 $b_1 = a_1, \cdots, b_r = a_r, b_{r+1} = {a_1}^{-1}, \cdots, b_{2r} = {a_r}^{-1}$. 则显然 G 中每个元素均可表成诸 b_i 的有限积．再设 $|G : H| = n$, 且 $1 = x_1, x_2, \cdots, x_n$ 为 H 在 G 中 n 个右陪集的一个完全代表系．对于任意的 i, j, 若 $x_i b_j \in Hx_k$, 则可令

$$x_i b_j = h_{ij} x_k, h_{ij} \in H, i = 1, \cdots, n; j = 1, \cdots, 2r.$$

最后证明 H 可由集合 $\{h_{ij}\}$ 生成．

§7.

1. 利用例 7.10, 并对 $|G|$ 用归纳法．

2. 区别 G 只有一个极大子群和 G 有多于一个极大子群两种情形．对前者利用 §3 第 14 题及极大子群是单群的条件证明 G 是 p^2 阶循环群；而对后者，设 M, N 是 G 的任二不同的极大子群，先证 $G = M \times N$, 再证 M, N 分别为素数阶循环群，于是 G 是 pq 阶循环群或 p^2 阶初等交换 p 群．

第 II 章

3. 设 Σ 是 N 的一个轨道．由第 2 题，对任意的 $x \in G$, Σ^x 也是 $N^x = N$ 的轨道．由 G 是传递作用，$\Omega = \bigcup\limits_{x \in G} \Sigma^x$. 于是 N 的每个轨道均与 Σ 等长．

4. 由 G 交换，$G_\alpha \trianglelefteq G$. 由第 3 题，$G_\alpha$ 的所有轨道等长．但 G_α 有一长为 1 的轨道，即 $\{\alpha\}$, 故 G_α 的所有轨道长均为 1. 于是 G_α 在 Ω 上作用平凡．又由作用的忠实性，得 $G_\alpha = 1$.

5. 若 $C_G(A) > A$, 则存在交换子群 $B > A$. 由第 4 题，有 $|A| = |\Omega|, |B| = |\Omega|$. 于是得 $A = B$, 矛盾．

6. 对任意的 $\alpha \in \Omega$, 以 α 为不动点的群元素有 $|G_\alpha|$ 个．设 $\Delta_1, \cdots, \Delta_t$ 是 G 在 Ω 上的全部轨道．则有

$$\begin{aligned}\sum_{x \in G} f_x &= \sum_{i=1}^{t} \sum_{\alpha \in \Delta_i} |G_\alpha| = \sum_{i=1}^{t} |\Delta_i||G_\alpha| \\ &= \sum_{i=1}^{t} |G : G_\alpha||G_\alpha| = \sum_{i=1}^{t} |G| = t|G|.\end{aligned}$$

7. 首先，由 $\alpha\in\Gamma$ 得 $\Gamma\neq\phi$. 对任意的 $\gamma\in\Gamma, n\in N_G(G_\alpha)$, 有

$$(\gamma^n)^{G_\alpha}=\gamma^{nG_\alpha n^{-1}n}=\gamma^{G_\alpha n}=\gamma^n,$$

即 $\gamma^n\in\Gamma$. 这说明 $N_G(G_\alpha)$ 把 Γ 变到 Γ, 因此可看成 Γ 上的作用. 最后证明 $N_G(G_\alpha)$ 在 Γ 上传递：任取 $\alpha,\gamma\in\Gamma$, 由 G 传递，可找到 $g\in G$ 使 $\alpha^g=\gamma$. 因为

$$\alpha^{gG_\alpha g^{-1}}=\gamma^{G_\alpha g^{-1}}=\gamma^{g^{-1}}=\alpha,$$

故 $gG_\alpha g^{-1}\leq G_\alpha$, 比较阶得 $gG_\alpha g^{-1}=G_\alpha$, 于是 $g\in N_G(G_\alpha)$.

8. 若存在 $\alpha\in\mathrm{Aut}(G)$ 使 $H_1{}^\alpha=H_2$, 则令 $\mu:H_1x\mapsto H_2x^\alpha,\sigma:P_1(g)\mapsto P_2(g^\alpha)$, 则满足 $\mu P_1(g)^\sigma=P_1(g)\mu$, 即 $P_1(G)$ 和 $P_2(G)$ 置换同构. 反过来，若 $P_1(G)$ 和 $P_2(G)$ 置换同构，则有 $\{H_1x \mid x\in G\}$ 到 $\{H_2x \mid x\in G\}$ 上的一一映射 μ 以及 $P_1(G)$ 到 $P_2(G)$ 上的同构映射 σ 满足 $\mu P_1(g)^\sigma=P_1(g)\mu$. 设 $\sigma:P_1(g)\mapsto P_2(g^\beta)$, 易验证 $\beta\in\mathrm{Aut}(G)$. 再设 μ 把 H_1 映到 H_2y. 于是对置换表示 P_1, 点 H_1 的稳定子群是 H_1; 而对置换表示 P_2, 点 H_2y 的稳定子群是 $y^{-1}H_2y$. 由 $P_1(G)$ 和 $P_2(G)$ 置换同构，应有 $H_1{}^\beta=y^{-1}H_2y$, 由此即得所需之结论. 读者还应注意找出在何处用了表示 P_1,P_2 的忠实性？

9. 考虑集合 $M=\{(Hg,y) \mid Hg\in\Omega,y\in cl(x),Hgy=Hg\}$. $(Hg,y)\in M$ 表示点 Hg 是 $\varphi(y)$ 的不动点，且 $y\in cl(x)$, 亦即 y 属于点 Hg 的稳定子群 H^g 和 $cl(x)$ 的交. 用两种方法计算 M 的势. 首先，由共轭元 $\varphi(y),\varphi(x)$ 应有同样多的不动点，得 $|M|=|\mathrm{fix}_\Omega(x)|\cdot|cl(x)|$. 又，$cl(x)$ 中稳定点 Hg 的元素个数应为 $|cl(x)\cap H^g|=|(cl(x)\cap H)^g|=|cl(x)\cap H|=f(x)$, 而 $|\Omega|=|G:H|$, 故又得 $|M|=|G:H|f(x)$. 结合两个等式，即得所需之结论.

10. 验证所有上三角矩阵的集合 P 在矩阵乘法和取逆矩阵之下封闭，从而 P 是 $GL(n,p)$ 的子群. 计算 P 的阶，证明 P 是 Sylow p 子群.

11. 考虑 G 对子群 P,H 的双陪集分解，证明存在一个双陪集 PxH, 其中包含 P 的右陪集的个数不是 p 的倍数. 于是 $|H:H\cap P^x|$ 与 p 互素，即 $H\cap P^x\in\mathrm{Syl}_p(H)$.

12. 设 $|G|=n, G=\{1=g_1,g_2,\cdots,g_n\}$. 考虑域 $GF(p)$ 上形式线性组合的集合

$$V=\Big\{\sum_{i=1}^n a_ig_i \ \Big|\ a_i\in GF(p),g_i\in G\Big\}.$$

规定

$$\sum_i a_i g_i = \sum_i b_i g_i \Longleftrightarrow a_i = b_i, i = 1, \cdots, n;$$
$$\sum_i a_i g_i + \sum_i b_i g_i = \sum_i (a_i + b_i) g_i;$$
$$a(\sum_i a_i g_i) = \sum_i (a a_i) g_i, a \in GF(p).$$

则 V 成为 $GF(p)$ 上 n 维向量空间, $g_1, \cdots, g_n$ 是它的一组基. 对于任意的 $g \in G$, 考虑 V 到 V 的映射

$$R(g) : \sum_i a_i g_i \mapsto \sum_i a_i (g_i g),$$

则 $R(g)$ 是 V 的满秩线性变换. 并且映射

$$R : g \mapsto R(g)$$

是 G 到 $GL(n, p)$ 中的单同态, 于是 $G \cong R(G) \leq GL(n, p)$. 再应用 10 题和 11 题.

16. 仿照命题 4.9 的证法.

17. 考虑 G 依共轭变换作用在 G 的所有非正规子群的集合上.

18. 仿照定理 3.9 的证法.

19. 用 N/C 定理.

20. 用 N/C 定理.

21. 对 $|G|$ 作归纳法. 设结论对所有阶 $< |G|$ 的群已经成立. 取 G 的 Sylow p 子群 $P_1, \cdots, P_k$ 满足 $P_1 \cap \cdots \cap P_k = 1$, 但其中任意 $k-1$ 个的交均 >1. 令 $D = P_2 \cap \cdots \cap P_k$, 有 $D > 1$ 但 $P_1 \cap D = 1$. 显然可设 $k \geq 3$, 故 $D \notin \mathrm{Syl}_p(G)$. 再令 $M = C_G(D)$. 由 P_i 交换, 有 $M \geq \langle P_2, \cdots, P_k \rangle$. 考虑商群 M/D. 由 $(P_2/D) \cap \cdots \cap (P_k/D) = 1$ 及归纳假设, 存在两个 Sylow p 子群 P_i, P_j 使 $P_i \cap P_j = D$. 令 $P_1 \cap M = Q \leq P \in \mathrm{Syl}_p(M)$. 由 Sylow 子群的共轭性, 有 $\tilde{P} \in \mathrm{Syl}_p(M)$ 使 $P \cap \tilde{P} = D$. 这时有 $P_1 \cap P \cap \tilde{P} = 1$, 于是 $(P_1 \cap P) \cap (P_1 \cap \tilde{P}) = 1$. 因 $P_1 \cap \tilde{P} \leq P_1 \cap M = P$, 又显然 $P_1 \cap \tilde{P} \leq P_1$, 故 $P_1 \cap \tilde{P} \leq P_1 \cap P$. 由此得 $P_1 \cap \tilde{P} = 1$.

22. 设 $P \in \mathrm{Syl}_p(G)$. 若 $P \trianglelefteq G$, 则显然 G 可解. 若 $P \ntrianglelefteq G$, 则必有 $p=3$ 或 7. 考虑 G 在 P 上的置换表示, 证明 G/P_G 可解, 从而得到 G 可解.

23. 不妨设 $p > q$. 若 Sylow p 子群 $P \ntrianglelefteq G$, 则 $N_G(P) = C_G(P) = P$, 应用 Burnside 定理得 G 的 Sylow q 子群正规.

24. 设 $p < q, Q \in \mathrm{Syl}_q(G)$. 若 $Q \ntrianglelefteq G$, 则 $n_q(G) = p^2$, 并且 $q \mid p^2 - 1$. 由 $p < q$ 只能有 $p = 2, q = 3$. 再设 $P \in \mathrm{Syl}_2(G)$, 也假定 $P \ntrianglelefteq G$. 则 P 必非循环 (若否, G 有正规 2- 补, 即 $Q \trianglelefteq G$), 且 Q 必为 3^3 阶非交换群 (若否, 用 Burnside 定理可得 $P \trianglelefteq G$). 于是 $|Z(Q)| = 3$. 考虑 G 在 Q 上的置换表

示，得 $G/Q_G \lesssim S_4$，于是 $G/Q_G \cong A_4$. 这推出 $|Q_G| = 9$，并有 $Z(Q) \le Q_G$. (因 $Q_G \trianglelefteq Q$，$Z(Q)$ 是 Q 的唯一的 3 阶正规子群，故必含于 Q_G). 对 $Z(Q)$ 用 N/C 定理，得

$$N_G(Z(Q))/C_G(Z(Q)) \lesssim Z_2.$$

而 $C_G(Z(Q)) \ge Q$，又注意到 G 中没有指数为 2 的子群，(若有这样的子群 K，则由 $|K|$=54 有 Q char $K, K \trianglelefteq G$，于是 $Q \trianglelefteq G$)，这就迫使 $N_G(Z(Q)) = C_G(Z(Q)) = G$ 或 Q. 若 $C_G(Z(Q)) = G$，则 $Z(Q) \le Z(G)$. 考虑 $\overline{G} = G/Z(Q)$，由 $|\overline{G}| = 2^2 \cdot 3^2$ 推知 $\overline{G}$ 有正规 Sylow 子群，从而设法推出 G 也有正规 Sylow 子群. 故必有 $C_G(Z(Q)) = Q = N_G(Z(Q))$. 这时 $Z(Q)$ 有 4 个共轭子群，并都含于 Q_G. 于是 Q_G 为 9 阶初等交换 3- 群. 考虑 P (作为初等交换 2- 群) 在 Q_G 的 4 个 3 阶子群上的共轭作用，它是传递的，因而是正则的. 任取 $1 \ne x \in P$，有 $o(x) = 2$. 再取 $1 \ne a \in Q_G$，令 $a^x = b$，则 $\langle a \rangle \ne \langle b \rangle$. 但 $b^x = a^{x^2} = a$，于是有 $(ab)^x = a^x b^x = ba = ab$. 由 $\langle a \rangle \ne \langle b \rangle$ 知 $ab \ne 1$，故 $\langle ab \rangle^x = \langle ab \rangle$，与 x 在 Q_G 的 3 阶子群上作用正则相矛盾.

假定 $p > q$，$S_4 \times Z_3$ 可作为反例.

25. 除掉 $|G| = p^a, p^a q, p^2 q^2, p^2 q^3 (p < q), pqr, \cdots$ 等已知可解的情形外，尚需处理 $|G| = 2\cdot 3^2\cdot 5, 2\cdot 3^2\cdot 7, 2\cdot 3^2\cdot 11, 2\cdot 3\cdot 5^2, 2^2\cdot 3\cdot 7, 2^2\cdot 3\cdot 11, 2^2\cdot 3\cdot 13, 2^2\cdot 5\cdot 7, 2^3\cdot 3^2, 2^3\cdot 5^2$ 等十种情形. 因 $3^2\cdot 5, 3^2\cdot 7, 3^2\cdot 11, 3\cdot 5^2$ 阶群可解，用定理 3.9 的方法可得前四种情形的可解性. 应用 Sylow 定理，对第 5, 8 种情形有 $n_7 = 1$; 对第 7 种情形有 $n_{13} = 1$; 对第 10 种情形有 $n_5 = 1$. 于是仅剩下 $|G| = 2^2 \cdot 3 \cdot 11$ 和 $2^3 \cdot 3^2$ 两种情形. 对前者，若 $n_{11} = 12$，则由 Burnside 定理，G 有正规 11 补，于是 G 可解; 而对后者，若 $n_3 \ne 1$，则 $n_3 = 4$，考虑 G 在其 Sylow 3 子群的正规化子上的置换表示，即可得 G 之可解性.

26. A_5 和 $GL(3,2)$ 分别为 60 阶和 168 阶单群，(后者可参看研究题 11)，而 $A_5 \times Z_2$ 和 $A_5 \times Z_3$ 分别为 120 阶和 180 阶非可解群. 又，例 5.13 中已证没有 180 阶单群，故只须证没有 120 阶单群. 设 G 为 120 阶单群，则 $n_5 = 6$. 在 5 阶群的正规化子上作置换表示，得 $G \lesssim S_6$. 因 G 是单群，其元素不能对应于奇置换，故 $G \lesssim A_6$. 于是 A_6 有指数为 3 的子群，这与 A_6 是单群矛盾.

27. 由 Sylow 定理，$n_7 = n_{13} = 1$，于是 G 中有 91 阶循环正规子群 $\langle a \rangle$. 设 $\langle b \rangle$ 是 G 的 5 阶子群，则 b 在 $\langle a \rangle$ 上的作用相当于 $\langle a \rangle$ 的一个自同构 β. 显然只能有 $o(\beta)$=1 或 5. 但因

$$\mathrm{Aut}(\langle a \rangle) \cong Z_{\varphi(7)} \times Z_{\varphi(13)} \cong Z_6 \times Z_{12},$$

其中无 5 阶元，故 $\beta = 1$. 这推出 a, b 可交换，G 为循环群.

28. 若所有 n 阶群皆循环，则 n 不能有平方因子. 假定 $(n, \varphi(n)) > 1$，则存在 n 的二素因子 p, q 使得 p 整除 $\varphi(q) = q - 1$. 于是有 pq 阶非循环群

$G=\langle a,b\rangle, a^q=1, b^p=1, b^{-1}ab=a^r, r\not\equiv 1(\mathrm{mod}\ q), r^p\equiv 1(\mathrm{mod}\ q)$. 当然也有 n 阶非循环群，矛盾.

反之，若 $(n,\varphi(n))=1$, 则显然 n 无平方因子. 设 p 是 n 的最小素因子，则由 Burnside 定理，n 阶群 G 必 p 幂零. 令 $n_1=n/p$, 当然也有 $(n_1,\varphi(n_1))=1$. 由归纳法可得 n_1 阶群循环，即 G 有循环的正规 p 补 N. 再仿照 27 题证明 p 阶群在 N 上作用平凡，于是 G 为循环群.

29. 若 $p\nmid |\mathrm{Aut}(G)|$, 自然更有 $p\nmid |\mathrm{Inn}(G)|$. 于是 G 之 Sylow p 子群 $P\leq Z(G)$. 由 Burnside 定理推出 G 必 p 幂零. 设 N 是 G 的正规 p 补，有 $G=P\times N$. 于是 $\mathrm{Aut}(G)\cong \mathrm{Aut}(P)\times\mathrm{Aut}(N)$, 因 $|P|\geq p^2$, 故 $|\mathrm{Aut}(G)|\geq p$, 矛盾.

30. 设 G 为单群. 因 $1008=2^4\cdot 3^2\cdot 7$, 由 Sylow 定理，n_7=8 或 36. 设 $P\in \mathrm{Syl}_7(G)$, 若 $n_7=8$, 则 $|N_G(P)|=2\cdot 3^2\cdot 7$. 由 N/C 定理，$3\mid |C_G(P)|$, 于是 G 中有 21 阶元. 考虑 G 在 $N_G(P)$ 上的置换表示，得 $G\lesssim S_8$. 但 S_8 中无 21 阶元素，矛盾. 而若 $n_7=36$, 则 $|N_G(P)|=28$. 由 N/C 定理及 Burnside 定理，可得 $|C_G(P)|=14$. 在 $C_G(P)$ 中取一 14 阶元 x, 则 $x^2\in P, o(x^2)=7$. 再考虑 G 在 $N_G(P)$ 上的置换表示 φ, 由推论 4.12, 知 $\varphi(x^2)$ 为五个 7- 轮换之积. 注意到 $\varphi(G)$ 中无奇置换，推知 $\varphi(x)$ 为两个 14 轮换和一个 7 轮换的积. 于是 $\varphi(x^7)$ 有 8 个不动点. 由命题 4.13, 对于 $N_G(P)-C_G(P)$ 中的任意元素 $y,\varphi(y)$ 的不动点数 ≤ 6, 这推出 x^7 与 y 不共轭. 又因 $C_G(P)$ 中只有一个 2 阶元 x^7, 故在 $N_G(P)$ 中，与 x^7 共轭的元素仅为 x^7 自身，应用第 9 题，有

$$|cl(x^7)|=\frac{|G:N_G(P)|f(x^7)}{|\mathrm{fix}_{\ \Omega}(x^7)|}=\frac{36\cdot 1}{8}=\frac{9}{2},$$

因 $|cl(x)|$ 是整数，矛盾.

31. 设 G 不可解，证明 G 必为非交换单群. 再用定理 5.7, 推知 $|G|=2^r\cdot 3\cdot r$. 最后若 $r>5$, 则 $n_r(G)=1$, 与 G 是单群矛盾.

第 III 章

6. 对 H 关于 G 的合成长度 $l_G(H)$ 作归纳法. 于是可设有 G 的子群 K 满足 $H\trianglelefteq K\trianglelefteq G$. 任取 $x\in G$, 则 $H^x\leq K$, 并且 $H^x\trianglelefteq K$. 于是 $\langle H,H^x\rangle=HH^x$. 计算 $|HH^x|$:

$$|HH^x|=\frac{|H||H^x|}{|H\cap H^x|}=\frac{|H|^2}{|H\cap H^x|}.$$

故 $|HH^x|$ 的素因子也都是 $|H|$ 的素因子. 由 H 是 Hall 子群，即得 $|HH^x|=|H|$, 于是 $|H|=|H\cap H^x|$, 由此得 $H=H^x$. 由 x 的任意性得 $H\trianglelefteq G$.

7. 首先，易看出若 $A \lhd \lhd G, A \leq H \leq G$, 则 $A \lhd \lhd H$. 于是不失普遍性，可令 $G = \langle A, B \rangle$.

又，若 A, B 中有一个是 G 的正规子群，譬如 $A \trianglelefteq G$, 则 $G = AB$. 由 $(|A|, |B|) = 1$, 知 B 为 G 之次正规 Hall 子群，由第 6 题， $B \trianglelefteq G$, 于是 $G = A \times B$, 结论成立.

对于一般的情形我们用对 $|G : A|$ 的归纳法. 并可假定 $A \ntrianglelefteq G$. 由 $A \lhd \lhd G$, 总可找到 G 的子群 H, K 使 $A \trianglelefteq H \trianglelefteq K$, 但 $A \ntrianglelefteq K$. 于是存在 $x \in K$ 使 $A^x \neq A$. 但 $A^x \trianglelefteq H$, 有 $\langle A, A^x \rangle = AA^x$, 并且 $|AA^x| > |A|$. 计算 $|AA^x|$, 由 $(|A|, |B|) = 1$ 可推得 $(|AA^x|, |B|) = 1$. 但 $|G : AA^x| < |G : A|$. 由归纳假设， $G = AA^x \times B$, 于是 $B \trianglelefteq G$, 结论成立. 证毕.

8. 注意，由 A, B 无公共合成因子及 $A \cap B$ 亦次正规，可得 $A \cap B = 1$. 不失普遍性，亦可设 $G = \langle A, B \rangle$.

假定 $A \trianglelefteq G$. 若亦有 $B \trianglelefteq G$, 则 $G = A \times B$, 结论成立. 若 $B \ntrianglelefteq G$, 则存在子群 H, K 使 $B \trianglelefteq H \trianglelefteq K$, 但 $B \ntrianglelefteq K$. 取 $x \in K$ 使得 $B^x \neq B$. 则 $\langle B, B^x \rangle = BB^x$. 易验证 BB^x 只含有 B 中的合成因子，于是 $BB^x \cap A = 1$. 这时由 $G = AB = A(BB^x)$ 推出 $|G| = |A||B| = |A||BB^x|, |B| = |BB^x|$, 与 $B \neq B^x$ 矛盾.

对于一般的情形，仍用对 $|G : A|$ 的归纳法. 仿照第 7 题提示的方法完成证明.

10. 令 $a = (123), b = (124), c = (125)$, 则 $A_5 = \langle a, b, c \rangle$, 且 $(ab)^2 = (bc)^2 = (ca)^2 = (ba)^2 = (cb)^2 = (ac)^2 = 1$. 设 $\mu \in \mathrm{Aut}(A_5)$, 则因 a^μ, b^μ, c^μ 仍为 3 阶元，故仍为 3- 轮换. 再由 $(a^\mu b^\mu)^2 = (b^\mu c^\mu)^2 = (c^\mu a^\mu)^2 = (b^\mu a^\mu)^2 = (c^\mu b^\mu)^2 = (a^\mu c^\mu)^2 = 1$, 推知 a^μ, b^μ, c^μ 必有形状：

$$a^\mu = (ijk), b^\mu = (ijl), c^\mu = (ijm),$$

其中 i, j, k, l, m 为 1,2,3,4,5 的一个排列. 令

$$d = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i & j & k & l & m \end{pmatrix}, \text{则}$$
$$a^\mu = d^{-1}ad, b^\mu = d^{-1}bd, c^\mu = d^{-1}cd.$$

又因 $A_5 = \langle a, b, c \rangle$, 故 μ 在 A_5 上的作用相当于 d 在 A_5 上的共轭作用.

另一方面， S_5 的任一元素都在 A_5 上诱导出一个自同构. 并且因 $C_{S_5}(A_5) = 1$, S_5 的不同元素诱导出的自同构也不相同. 于是得 $\mathrm{Aut}(A_5) \cong S_5$.

11. 由条件， G 有正规子群 $N \cong A_5$, 且 $G/N \cong A_5$. 对 N 用 N/C 定理得

$$G/C_G(N) \lesssim \mathrm{Aut}(N) \cong S_5.$$

由此推得 $G/C_G(N) \cong A_5, C_G(N) \cong A_5$. 因 A_5 是单群, $C_G(N) \cap N = 1$, 故 $G = C_G(N) \times N \cong A_5 \times A_5$.

15. 因 $Z(A \times B) = Z(A) \times Z(B)$, 由 p 群中心非平凡, 立得结论.

16–18. 所有这些群均系可解群. 仿照例 3.12 应用群扩张理论逐一决定之.

19. 设 $\overline{G} = G/Z(G)$ 是广义四元数群, 则 $\overline{G} = \langle \bar{a}, \bar{b} \rangle$, 有关系 $\bar{a}^{2m} = \bar{1}, \bar{b}^2 = \bar{a}^m, \bar{b}^{-1}\bar{a}\bar{b} = \bar{a}^{-1}$. 再设 a, b 是 $\bar{a}, \bar{b}$ 的原像. 则 $G = \langle a, b, Z(G) \rangle$. 由关系式 $\bar{b}^2 = \bar{a}^m$ 推出 $a^m = b^2 z$, 其中 $z \in Z(G)$. 这推出 a^m 与 b 可交换, 即 $a^m \in Z(G)$. 于是 $\bar{a}^m = \bar{1}$, 矛盾.

20. 因 $N \trianglelefteq G$, 有 $NK \leq G$. 由 $NK \cdot H = G$, 计算阶, 得

$$|G| = \frac{|N||K||H|}{|NK \cap H|},$$

由此推出 $|K| = |NK \cap H|$. 于是在 NK 中, K 和 $NK \cap H$ 是 N 的两个补. 由定理 4.3, 有 $n \in N$ 使 $n^{-1}Kn = NK \cap H$, 于是得 $n^{-1}Kn \leq H$.

21. 设 $X \in M_n(G)$, g_i 是 X 的第 i 行中的非 0 元素. 令 $D(X) = \mathrm{diag}(g_1, \cdots, g_n)$, 即对角元素依次为 $g_1, \cdots, g_n$ 的 n 级对角矩阵; 再令 $H(X)$ 为把 X 中所有非 0 元素均换成 1 得到的矩阵, 它是置换矩阵. 则有 $X = D(X) \cdot H(X)$. 令

$$H = \{H(X) \mid X \in M_n(G)\}, N = \{D(X) \mid X \in M_n(G)\}.$$

则 $H \cong S_n$, 而 $N \cong \underbrace{G \times \cdots \times G}_{n\ 个}$. 最后验证 $H(X)$ 在 N 上的共轭作用相当于定义圈积时 $\alpha(h)$ 在 $G \times \cdots \times G$ 上的作用, 其中 h 为对应于置换矩阵 $H(X)$ 的置换.

25. 计算正则圈积的阶.

26. 注意正则圈积和圈积的情况是完全不同的. 为证明正则圈积的情形, 首先应弄清 G 与 H 的正则圈积的构造和乘法规律. 令 $|H| = n$, 且 $H = \{1, h_2, \cdots, h_n\}$, 则

$$G \wr_r H = \{(g_1, \cdots, g_{h_n}; h) | g_{h_i} \in G, h \in H\},$$

乘法如下进行:

$$(g_1, \cdots, g_{h_n}; h)(g'_1, \cdots, g'_{h_n}; h') = (g_1 g'_{1^h}, \cdots, g_{h_n} g'_{h_n{}^h}; hh').$$

注意在上式中 H 的元素作为 G 的元素的脚标. 现在令 $|H_1| = m, |H : H_1| = k$, 并作陪集分解

$$H = \bigcup_{i=1}^{k} x_i H_1, 其中, x_1 = 1.$$

设 $H_1 = \{1, h_2, \cdots, h_m\}$, 则 H 的元素可表成

$$H = \{1, h_2, \cdots, h_m, x_2, x_2h_2, \cdots, x_2h_m, \cdots, x_k, x_kh_2, \cdots, x_kh_m\}.$$

按照 H_1 和 H 的元素的上述次序写出 $G_1 \wr_r H_1$ 和 $G \wr_r H$ 的元素的一般形状, 再设法找出所需之单同态.

27. 计算 $G \wr H$ 和 $G_p \wr H_p$ 的阶.

28. 生成元为 (1 2 3), (1 4 7)(2 5 8)(3 6 9) 和 (1 10 19)(2 11 20)(3 12 21)(4 13 22)(5 14 23)(6 15 24)(7 16 25) (8 17 26)(9 18 27).

30. 从内循环群中选出同时亦为外循环群者.

第 IV 章

1. 首先证 AB 是 G 的子群, 然后用命题 1.2(4).

3. (1) 先验证该映射确为同态. 再令 x^ia, x^jb 为 G 中任二元素, 其中 $a, b \in A$, 设法用换位子公式 (命题 1.2) 把 $[x^ia, x^jb]$ 化成 $[c, x]$ 形状, 其中 c 为 A 的某一适当的元素.

(2) 用同态基本定理.

4. 用第 3 题 (1), 映射 $a \mapsto [a, x], a \in G'$, 是 G' 到 G' 上的满同态. 再由 G 之有限性, 知该映射为 G' 之自同构. 设 $x^n \in G'$, 则上述映射把 x^n 映到 $[x^n, x] = 1$, 于是必有 $x^n = 1$.

5. (1)–(4): 用命题 1.2 及 G' 的交换性.

(5) 由 (4) 及 $c \in G'$, 有

$$[b, c, a][c, a, b] = 1,$$

于是 $[c, a, b] = [b, c, a]^{-1} = [[b, c]^{-1}, a] = [c, b, a]$.

6. 用定理 1.8(2) 及第 5 题 (5).

7. 设 $G = \langle a, b\rangle$, 则 $G = \langle [a, b], G_3\rangle$. 令 $G_5 = 1$, 我们来证 $G'' = 1$. 计算 G' 中任二元素的换位子, 并注意到 $[G', G_3] = [G_2, G_3] \leq G_5 = 1$.

11. 证必要性时应用定理 2.7(4). 证充分性时分析使定理不真的极小反例 G, 因为定理条件是子群遗传的, 于是 G 是内幂零群. 最后由内幂零群的结构导出矛盾.

12. 应用第 11 题.

13. (4) 若 G/N_1 和 G/N_2 都是 p 群, 则因

$$G/N_1 \cap N_2 \lesssim (G/N_1) \times (G/N_2),$$

$G/N_1 \cap N_2$ 亦为 p 群.

15. (3) 因 $G/O^p(G)$ 幂零, 故 $G_\infty \le O^p(G)$. 于是 $G_\infty \le \bigcap_{p||G|} O^p(G)$. 为证另一包含关系，我们令 $H = G_\infty$. 因 G/H 幂零，故对任意的素数 $p \bigm| |G|$, G/H 有正规 p 补 C_p/H, 且显然有 $\bigcap_{p||G/H|} C_p/H = 1$, 于是 $\bigcap_{p||G/H|} C_p \le H$. 因 $G/C_p \cong (G/H)\big/(C_p/H)$ 是 p 群，故 $C_p \ge O^p(G)$. 于是 $\bigcap_{p||G/H|} O^p(G) \le H$, 自然更有 $\bigcap_{p||G|} O^p(G) \le H$.

(4) 由 $G_\infty = G_n = G_{n+1} = \cdots$, 有

$$G_\infty = G_{n+1} = [G_n, G] = [G_\infty, G],$$

故 $G_\infty \le \langle N \trianglelefteq G \bigm| [N,G] = N\rangle$. 反过来，设 $N \trianglelefteq G, [N,G] = G$. 则

$$N = [N,G] = [N,G,G] = \cdots = [N,\underbrace{G,\cdots,G}_{n\ 个}] \le G_\infty,$$

得另一包含关系.

17. 因 G 是有限群，故存在正整数 n 使得

$$Z_\infty(G) = Z_n(G) = Z_{n+1}(G) = \cdots,$$

于是 $Z(G/Z_\infty(G)) = Z(G/Z_n(G)) = Z_{n+1}(G)/Z_n(G) = 1$. 故 $Z_\infty(G) \ge \bigcap\{N \bigm| N \trianglelefteq G\ 且\ Z(G/N) = 1\}$. 为证另一包含关系，只须证由 $N \trianglelefteq G, Z(G/N) = 1$ 可推出 $Z_\infty \le N$. 因 $Z(G/N) = 1$, 有 $Z_n(G/N) = 1$, 即 $Z_n(G)N/N = 1$, 于是 $Z_n(G) \le N$. 但 $Z_n(G) = Z_\infty(G)$, 故 $Z_\infty(G) \le N$.

19. 用对 $|G|$ 的归纳法. 若 $Z(G) = 1$, 当然也有 $Z_\infty(G) = 1$, 此时结论显然成立. 故可设 $Z(G) \neq 1$, 考虑商群 $\overline{G} = G/Z(G)$. 易验证 $Z_\infty(\overline{G}) = Z_\infty(G)/Z(G)$. 由归纳假设有 $Z_\infty(\overline{G})\overline{A}$ 幂零，其中 $\overline{A} = AZ(G)/Z(G)$. 于是 $Z_\infty(G)A/Z(G)$ 幂零. 由此推得 $Z_\infty(G)A$ 亦幂零.

20. 任取 $S \in \mathrm{Syl}_p(G)$, 则 $P \le S$. 由 $G/C_G(P)$ 是 p 群，有 $G = C_G(P)S$. 令 $P_1 = [P,G]$, 有 $P_1 \trianglelefteq G$, 且 $P_1 \le P$. 因 $G = C_G(P)S$, 有

$$P_1 = [P,G] = [P, C_G(P)S] = [P,S] < P,$$

并且 $C_G(P_1) \ge C_G(P)$, 于是 $G/C_G(P_1)$ 仍为 p 群. 再令 $P_2 = [P_1, G], P_3 = [P_2, G], \cdots$. 同法可证必存在正整数 k 使 $P_k = 1$, 即

$$[P,\underbrace{G,\cdots,G}_{k\ 个}] = 1.$$

由此推得 $P \le Z_k(G) \le Z_\infty(G)$.

21. 对任意正整数 n, 由 G/G_n 幂零, 据 11 题可得 $[x,y]\in G_n$. 由 n 的任意性得

$$[x,y]\in\bigcap_{i=1}^{\infty}G_n=G_\infty.$$

但因 $G_\infty=1$, 故 $[x,y]=1$.

22. 设 $\exp(Z_i(G)/Z_{i-1}(G))=n, a\in Z_{i+1}(G)$, 我们要证明 $a^n\in Z_i(G)$. 这只要证对任意的 $g\in G$, 有 $[a^n,g]\in Z_{i-1}(G)$. 因 $[a,g]\in Z_i(G)$, 故有 $[a,g]^n\in Z_{i-1}(G)$. 设法用换位子公式由此条件推出 $[a^n,g]\in Z_{i-1}(G)$.

本题第二部分证明方法与上面相同.

23. 设 $x\in Z_2(G)$, 则对任意的 $g,h\in G$ 有

$$[x,g^{-1},h]^g=1,[h,x^{-1},g]^x=1.$$

由 Witt 公式即得 $[g,h^{-1},a]^h=1$, 于是 $[a,[g,h^{-1}]]=1$. 由 g,h 的任意性有 $a\in C_G(G')$. 但 $G'=G$, 故得 $a\in Z_1(G)$.

为造本题第二部分所要求的例子, 先任取一有限幂零群 N, 其幂零类 $c(N)=n$. 设 $|N|=m$, 令 V 为在域 $GF(2)$ 上以 N 的元素为基的 m 维向量空间的加法群. N 的右正则表示的像 $R(N)$ 可看作 V 的一个自同构群. 作 V 和 $R(N)$ 的半直积 G, 验证 G 即满足本题的要求.

25. 下面的群 G 可作为本题需要的例子:

$$G=\langle a,b\rangle:a^5=1,a^4=1,b^{-1}ab=a^2.$$

取 $N=\langle a\rangle$, 有 $\Phi(G/N)\cong Z_2$; 但 $\Phi(G)=1,\Phi(G)N/N=1$.

26. 因为 $G_i\trianglelefteq G_1\times G_2, i=1,2$, 故由推论 3.5 有 $\Phi(G_i)\le\Phi(G_1\times G_2)$, 于是得 $\Phi(G_1)\times\Phi(G_2)\le\Phi(G_1\times G_2)$. 为证相反的包含关系, 只需考虑 $G_1\times G_2$ 的形如 $M_1\times G_2$ 和 $G_1\times M_2$ 的极大子群, 其中 M_i 是 G_i 的极大子群, i=1,2. 证明所有这种类型的极大子群的交已经为 $\Phi(G_1)\times\Phi(G_2)$.

27. 用定理 4.2 的结论和定理 4.3 的证明方法. 为造反例考虑四元数群 Q 和 9 阶循环群 $\langle a\rangle$ 的半直积 $Q\rtimes\langle a\rangle$, a 在 Q 上的作用相当于 Q 的下述自同构: 设 $Q=\langle x,y\rangle$, 满足关系 $x^4=1,y^2=x^2,y^{-1}xy=x^{-1}$, 则 $x^a=y,y^a=xy$. 证明这个自同构是 3 阶的, 于是 $a^3\in Z(G)$. 又, G 中仅有一个 2 阶元 $x^2=y^2$, 它也在 G 的中心中. 再用 Sylow 定理证明 G 仅有一个 3 阶子群, 即 $\langle a^3\rangle$.

28. 在定理 4.2 给出的内幂零群的构造的基础上找出它同时为外幂零群应满足的条件.

29. 参看定理 4.2 给出的内幂零群的构造, 只须证若 $p=2$, 也有 $\exp P=2$. 因这时仍有

$$P=\langle[x,y]\mid x\in P,y\in Q\rangle\ 和\ [x^2,y]=1,$$

又 P 是交换群，故只须证 $[x,y]^2=1$. 但

$$[x,y]^2=(x^{-1}x^y)^2=x^{-2}(x^2)^y=[x^2,y]=1.$$

30. (2) 设 $|G|=p^n$, 取 G 的二极大子群 M_1 和 M_2, 令 $N=M_1\cap M_2$. 证明 $N=Z(G)$, 且 G/N 为 (p,p) 型交换群. 于是由 (1) 必有 $N=\Phi(G)$.

31. 因 G 非交换，可取到 G 的子群 H 为内交换群. 区分 H 为 p 群和非 p 群两种情形，应用第 29 题和第 30 题.

32. 考虑商群 $G/\mho(G)$, 证明其交换，于是 $G'\le\mho(G)$.

33. (2) 对 A 用 N/C 定理，由 (1) 得 $G/A\lesssim\mathrm{Aut}(A)$. 设 $d(A)=d$, 由定理 5.3 有

$$|\mathrm{Aut}(A)|\ \Big|\ p^{d(a-d)}(p^d-1)(p^d-p)\cdots(p^d-p^{d-1}).$$

于是 $|G/A|\le p^{d(a-d)}\cdot p^{1+2+\cdots+(d-1)}$. 由此推出

$$n\le d(a-d)+\frac{d(d-1)}{2}+a,$$

再设法证明上不等式右端 $\le\frac{a(a+1)}{2}$.

(3) 由 $A\le Z_a(G)$ 及 $[G_a,Z_a(G)]=1$ 推出 $G_a\le C_G(A)=A$.

(4) 令 $B=\langle A_1,A_2\rangle$, 有 $A_1\cap A_2\le Z(B)$. 设法证明 $B'\le Z(B)$, 于是 $c(B)\le 2$. 据第 22 题， $\exp(B/Z(B))$ 整除 $\exp(Z(B))$, 于是有 $\exp B\le(\exp(Z(B)))^2$. 由此得

$$\exp A_2\le\exp B\le(\exp(Z(B)))^2\le(\exp A_1)^2,$$

即 $a_2\le 2a_1$.

34. 考虑 p^a 阶初等交换 p 群 A 的全形. 证明其中有 $p^{\frac{a(a+1)}{2}}$ 阶子群 $G=A\rtimes B$. 再证 $C_G(A)=A$, 于是 A 是 G 的极大交换正规子群.

35. 若 G 交换，则结论显然不成立. 若 G 不交换，则二交换极大子群的交是 $Z(G)$, 且 $G/Z(G)$ 是 (p,p) 型交换群. 设 $\overline{M}$ 是 $G/Z(G)$ 的任一 p 阶子群，则 M 是 G 的交换极大子群.

37. 设 A 是 G 的交换子群，且 $A\ntrianglelefteq G, |G:A|=p^2$. 取 G 的极大子群 $B>A$. 若 B 交换，则任取 B 的在 G 中正规的极大子群即为所求. 故可设 B 非交换. 因 $B\trianglelefteq G, A\ntrianglelefteq G$, 故存在 $x\in G$ 使 $A^x\ne A$, 这时必有 $B=\langle A^x,A\rangle, Z(B)=A^x\cap A$, 且 $B/Z(B)$ 为 (p,p) 型群. 在 B 中任取一在 G 中正规的极大子群即可满足本题的要求.

第 V 章

2. 用归纳法. 取 G 的一个极小正规子群 N, 则 N 是 π 群或 π' 群. 区分 $N \le M$ 和 $N \not\le M$ 两种情形证明之. 前者考虑商群 G/N, 用归纳假设; 后者利用等式 $G = NM$.

3. 用反证法. 设 H 不是 G 的 Hall 子群, 则存在素数 $p \mid |H|$ 以及 $P_1 \in \mathrm{Syl}_p(H), P \in \mathrm{Syl}_p(G)$ 使得 $1 < P_1 < P$. 取 $1 \ne x \in Z(P)$, 证明 $x \in P_1$, 但 $C_G(x) \not\le H$, 矛盾.

4. 设 G 为 π- 可解, 则 G 的每个子群亦 π 可解. 特别地, G 的 π-Hall 子群 π- 可解, 于是它必可解. 反过来, 由 π-Hall 子群可解推出 G 必 π- 可解用对 $|G|$ 的归纳法. 任取 G 的极小正规子群 N, 证明 N 或为 π'- 群, 或为 p- 群, 其中 $p \in \pi$. 然后用归纳假设.

5. 因 $N_G(A) \ge C_G(A), N_G(A) \ge P$, 若在 $N_G(A)$ 中考虑, A 是正规子群, 且 $C_{N_G(A)}(A) = C_G(A)$. 故不失普遍性, 可令 $A \trianglelefteq G$. 再证明 $A \in \mathrm{Syl}_p(C_G(A))$. 最后用 Schur-Zassenhaus 定理证明 A 在 $C_G(A)$ 中有补 $O_{p'}(C_G(A))$, 且 $C_G(A) = A \times O_{p'}(C_G(A))$.

6. 用反证法. 令 $C = C_G(O_\pi(G))$. 若 $C \not\le O_\pi(G)$, 则 $CO_\pi(G)/O_\pi(G) > 1$. 由 $CO_\pi(G) \trianglelefteq G$ 及 G 的 π 可分性, 存在 $1 < M/O_\pi(G) < CO_\pi(G)/O_\pi(G)$, 使 $M/O_\pi(G)$ 是 G/O_π 的 π' 正规子群. 用 Schur-Zassenhaus 定理, $O_\pi(G)$ 在 M 中有补 N, 且 $M = N \times O_\pi(G)$, N 是 π' 群. 易证 $N \trianglelefteq G$, 于是 $N \le O_{\pi'}(G)$, 与 $O_{\pi'}(G) = 1$ 矛盾.

7. 用第 6 题.

8. 令 $\overline{G} = G/\Phi(O_p(G))$, 先证明 $O_{p'}(\overline{G}) = \bar{1}$, 再应用第 6 题 (取 $\pi = \{p\}$).

9. (1) 由 G 为 p 可解及 $O_{p'}(G) = 1$ 知 $O_p(G) \ne 1$. 再用第 6 题.

(2) 由 $Z(P) \le C_G(O_p(G)) \le O_p(G)$ 立得.

(3) 由 (2) 及 $Z(O_p(G)) \trianglelefteq G$ 得 $Z(P)^G \le Z(O_p(G))$.

(4) 用 N/C 定理于 $O_p(G)$.

(5) 首先, 应熟知下列事实: ①循环 2 群及 2^n 阶 $(n \ge 3)$ 的二面体群的自同构群仍为 2 群; ②$2^n$ 阶 $n \ge 3$ 的二面体群中的 2^{n-1} 阶循环子群是唯一的, 且它的每个子群都是正规子群; 但 2^n 阶二面体群只有两个非循环的正规子群, 它们是 2^{n-1} 阶的二面体群 (对不熟悉上述事实的读者请先证明这些结论).

现在设 P 循环或为阶 ≥ 16 的二面体群, 则 $O_p(G)$ 循环或为阶 ≥ 8 的二面体群. 对 $O_p(G)$ 用 N/C 定理, 注意到第 6 题即得到 G 是 2 群, 从而 $G = P$.

再设 P 为 8 阶二面体群, 由 $O_p(G)$ 循环或 $O_p(G) = P$ 可推出 $G = P \lesssim S_4$; 而由 $O_p(G)$ 为 4 阶初等交换 2 群可推出 G 同构于 $O_p(G)$ 的全形

的子群，但 $O_p(G)$ 的全形同构于 S_4.

最后设 P 是四元数群，若 $O_p(G)$ 循环仍可推出 $G=P$, 矛盾，故必有 $O_p(G)=P$. 此时有 $G=O_{pp'}(G)$.

10. 设结论不真，并设 G 是最小阶反例. 取 G 的极小正规子群 N. 则

(1) $N\in \mathrm{Syl}_p(G)$: 由 G 可解，N 必为素数幂阶群. 若 $|N|=q^n, q\neq p$, 则 G/N 有 p 补 K/N, K 即为 G 之 p 补；若 $|N|=p^i, N\notin \mathrm{Syl}_p(G)$, 则同样 G/N 有 p 补 $K/N, K<G$. 由 G 的极小性，K 亦有 p 补 K_1, K_1 即为 G 之 p 补，都与 G 无 p 补相矛盾.

(2) 令 $\overline{G}=G/N$, M/N 是 $\overline{G}$ 的极小正规子群，则 M/N 是素数幂阶群. 譬如令 $|M/N|=q^s$, 有 $q\neq p$. 设 $Q\in \mathrm{Syl}_p(M)$, 则 $M=QN$. 用 Frattini 论断，有 $G=N_G(Q)M=N_G(Q)N$. 因 $Q\ntrianglelefteq G$, 故 $N_G(Q)<G$. 取 $N_G(Q)$ 的 p 补 K, 则 K 为 G 之 p 补. 矛盾.

11. 设 G 是使结论不真的最小阶反例，N 是 G 的任一极小正规子群. 若 N 是 π' 群，则结论对 G/N 成立. 再利用 Schur-Zassenhaus 定理即可得出矛盾. 若有 $p\in\pi, p\,\big|\,|N|$, 令 $P\in \mathrm{Syl}_p(N)$. 如果 $P=N$, 考虑商群 G/N 易推出结论对 G 成立，矛盾. 如果 $P\neq N$, 则 $P\ntrianglelefteq G, N_G(P)<G$. 令 M 是 N 的 π'-Hall 子群，由 Frattini 论断，有 $G=N_G(P)N=N_G(P)PM=N_G(P)M$. 易验证 $N_G(P)$ 的主因子的阶仍至多含 π 中一个素因子，于是结论对 $N_G(P)$ 成立. 但 $N_G(P)$ 的 π-Hall 子群 H 亦为 G 之 π-Hall 子群. 故 G 中存在可解 π-Hall 子群 H. 再设 H_1 是 G 的另一 π-Hall 子群. 令 $P_1=H_1\cap N$, 证明 $P_1\trianglelefteq H_1$, 且 $P_1\in \mathrm{Syl}_p(N)$. 由 Sylow 定理，存在 $x\in N$ 使 ${P_1}^x=P$. 于是 $P\trianglelefteq {H_1}^x$, 即 ${H_1}^x\leq N_G(P)$. 由 G 之极小性得 H 和 ${H_1}^x$ 在 $N_G(P)$ 中共轭，于是 H 和 H_1 在 G 中共轭，矛盾.

12. 考虑 Sylow 系和 Sylow 补系的关系.

14. 仿照 II,2.5 和 II,2.6 的证明. 并适当推广 Frattini 论断 (II,2.4).

15. 由 $F(G)$ 是 p 群推知 $O_{p'}(G)=1, F(G)=O_p(G)$. 于是 $O_p(G/F(G))=1$, 故 $F(G/F(G))$ 是 p' 群.

16. 用定理 4.5(2).

17. 用定理 4.5(2) 及 $F(G)$ 的定义.

18. 若 G 中有一 4 阶子群或 3 阶子群是正规的，则 G 在存在 12 阶子群. 若否，则 $x^4=1$ 在 G 中至少有 8 个解，$x^3=1$ 在 G 中至少有 6 个解. 与 $x^{12}=1$ 恰有 12 个解相矛盾.

第 VI 章

3. 设 V 是对应置换表示 $\mathbf{P}$ 的 G 空间，并设 $v_1,\cdots,v_n$ 是 V 的一组基. 证明 $\langle v_1+\cdots+v_n\rangle$ 是 V 的一维 G 子空间.

4. 令 $\mathbf{S}=\sum_{a\in G}\mathbf{X}(a)$, 验证 $\mathbf{S}\ \mathbf{X}(t)=\mathbf{X}(t)\mathbf{S}, \forall t\in G$. 由 Schur 引理, $\mathbf{S}=\lambda\mathbf{I}, \lambda\in\mathbb{C}$. 应用第一正交关系, $\mathbf{X}$ 对应的特征标 χ 和主特征标 1_G 的内积为 0, 即 $\langle\chi, 1_G\rangle=0$. 但

$$\langle\chi, 1_G\rangle=\frac{1}{g}\sum_{a\in G}\chi(a)=\frac{1}{g}\mathrm{tr}\ \mathbf{S},$$

故推得 $\lambda=0$.

5. 应用第 3 题.

7. 设 $\mathbf{X}$ 是对应于特征标 χ 的 G 的矩阵表示. 对于任意复矩阵 $\mathbf{A}=(a_{ij})$, 规定 $\mathbf{A}^\sigma=({a_{ij}}^\sigma)$. 考虑映射

$$\mathbf{X}^\sigma: a\mapsto\mathbf{X}(a)^\sigma, a\in G.$$

证明 $\mathbf{X}^\sigma$ 是 G 的表示, 且它对应的特征标为 χ^σ.

8. 设

$$\mathbf{A}=\begin{pmatrix} a_{11} & \cdots & a_{1m}\\ \vdots & & \vdots\\ a_{m1} & \cdots & a_{mm}\end{pmatrix} \text{ 和 } \mathbf{B}=\begin{pmatrix} b_{11} & \cdots & b_{1n}\\ \vdots & & \vdots\\ b_{n1} & \cdots & b_{nn}\end{pmatrix}$$

是任二复矩阵. 规定

$$\mathbf{A}\otimes\mathbf{B}=\begin{pmatrix} a_{11}\mathbf{B} & \cdots & a_{1m}\mathbf{B}\\ \cdots & & \cdots\\ a_{m1}\mathbf{B} & \cdots & a_{mm}\mathbf{B}\end{pmatrix},$$

叫做 $\mathbf{A}$ 和 $\mathbf{B}$ 的 Kronecker 积. 现在设 $\mathbf{X}, \mathbf{Y}$ 分别为对应于特征标 χ, ψ 的矩阵表示. 证明映射

$$\mathbf{X}\otimes\mathbf{Y}: a\mapsto\mathbf{X}(a)\otimes\mathbf{Y}(a), a\in G,$$

仍为 G 的表示, 并且有特征标 $\chi\psi$.

(2) 利用

$$\langle\chi\psi, 1_G\rangle=\frac{1}{g}\sum_{a\in G}\chi(a)\psi(a)=\frac{1}{g}\sum_{a\in G}\chi(a)\overline{\chi(a)}=\langle\chi,\chi\rangle.$$

9. 若 H 交换, H 的每个不可约特征标是线性的, 故 $\chi|_H$ 可表成 H 的线性特征标之和. 反之, 若 $\chi|_H$ 可表成线性特征标的和, 可推出 $H'\leq\mathrm{Ker}\ \chi|_H$. 但因 χ 是忠实的, 故 $H'=1$, 即 H 是交换群.

10. (1) 因 H 交换，χ 可分解为若干个线性特征标的和．设

$$\chi=\sum_{i=1}^{m}n_i\lambda_i,$$

其中 n_i 为正整数，$\lambda_1,\cdots,\lambda_m$ 为两两不同的 H 的线性特征标．则

$$\frac{1}{|A|}\sum_{a\in A}|\chi(a)|^2=\langle\chi,\chi\rangle=\langle\sum_{i=1}^{m}n_i\lambda_i,\sum_{i=1}^{m}n_i\lambda_i\rangle=\sum_{i=1}^{m}{n_i}^2.$$

因 $\sum\limits_{i=1}^{m}{n_i}^2\geq\sum\limits_{i=1}^{m}n_i=\chi(1)$, 故得所需之结论．

(2) 由

$$1=\langle\chi,\chi\rangle_G=\frac{1}{|G|}\sum_{a\in G}|\chi(a)|^2\geq\sum_{a\in A}|\chi(a)|^2\geq\frac{|A|}{|G|}\chi(1)$$

立得结论．

11. 设 G 是非交换单群，有二级不可约特征标 χ. 则因 $\chi(1)\mid|G|$, 知 $|G|$ 为偶数．于是 G 中有 2 阶元．若 G 只有一个 2 阶元，则它必属于中心 $Z(G)$, 与 G 是单群矛盾．故 G 至少有两个 2 阶元 a,b. 假定 $\mathbf{X}$ 是对应于 χ 的矩阵表示，则由 G 是单群，$\mathbf{X}$ 必为忠实表示，即 $\mathbf{X}(a)\neq\mathbf{X}(b)$. 再考虑第 1 题中给出的线性表示 $\det\mathbf{X}$. 由 G 是单群，$\det\mathbf{X}=1_G$. 于是 $\det\mathbf{X}(a)=\det\mathbf{X}(b)=1$. 最后，因 $\mathbf{X}(a),\mathbf{X}(b)$ 必相似于二级对角阵，且对角元素为 ±1, 考虑到 $\det\mathbf{X}(a)=\det\mathbf{X}(b)=1$ 及 $\mathbf{X}$ 的忠实性，有 $\mathbf{X}(a),\mathbf{X}(b)$ 相似于

$$\begin{pmatrix}-1 & \\ & -1\end{pmatrix}=-\mathbf{I},$$

因而必有 $\mathbf{X}(a)=-\mathbf{I},\mathbf{X}(b)=-\mathbf{I}$, 与 $\mathbf{X}(a)\neq\mathbf{X}(b)$ 矛盾．

12. 设 G 有二级不可约特征标 χ. 证明 $\chi|_{G'}$ 是 G' 的不可约特征标，应用第 11 题导出矛盾．

13. 若 a 和 a^{-1} 共轭，则 $\chi(a)=\chi(a^{-1})=\overline{\chi(a)}$, 于是 $\chi(a)$ 是实数．反之，若对 G 之任一特征标 χ, 恒有 $\chi(a)$ 为实数，即 $\chi(a)=\overline{\chi(a)}=\chi(a^{-1})$. 则由第二正交关系及

$$\sum_{\chi\in\mathrm{Irr}(G)}\chi(a^{-1})\overline{\chi(a)}=\sum_{\chi\in\mathrm{Irr}(G)}(\chi(a))^2>0$$

推知 a 和 a^{-1} 必共轭．

14. 设 $a \neq 1$ 是 G 中的实元素，且 $|G|$ 为奇数，则 $a \neq a^{-1}$，且存在 $b \in G$ 使 $b^{-1}ab = a^{-1}$. 由此推出 $b^{-2}ab^2 = a$，即 $b^2 \in C_G(a)$. 但因 $|G|$ 是奇数，$o(b)$ 亦为奇数，故得 $b \in C_G(a)$，即 $b^{-1}ab = a$，与 $a \neq a^{-1}$ 矛盾.

15. 设 $\mathbf{X}$ 是对应于 χ 的 G 的矩阵表示. 对于任意的 $t \in C_G(H)$，有 $\mathbf{X}(t)\mathbf{X}(h) = \mathbf{X}(h)\mathbf{X}(t), \forall h \in H$. 因 $\chi|_H$ 是 H 的不可约特征标，由 Schur 引理有 $\mathbf{X}(t) = \lambda\mathbf{I}, \lambda \in \mathbb{C}$. 于是 $\mathbf{X}(t) \in Z(\mathbf{X}(G))$. 由 $\mathbf{X}$ 是 G 的忠实表示，得 $t \in Z(G)$.

16. 由题设条件，可令 $\chi = \lambda 1_G, \lambda \in \mathbb{C}$. 因 χ 是 G 的特征标. 有 $\langle \chi, 1_G \rangle = \langle \lambda 1_G, 1_G \rangle = \lambda$ 是非负整数. 但显然 $\lambda \neq 0$，于是 λ 是正整数. 因此由 $\chi(1) = \lambda|G|$，得 $|G| \bigm| \chi(1)$.

17. (1) 由第一正交关系得

$$|G| = \sum_{a\in G} |\chi(a)|^2 \geq \sum_{a\in A} |\chi(a)|^2 =$$
$$|A|\langle \chi, \chi \rangle_A \geq |A|\chi(1) = |A||G:A| = |G|,$$

于是上式中“$\geq$”号全应为等号. 特别地，$\chi(a) = 0, \forall a \in G - A$.

(2) 选 $1 \neq a \in A$ 使 $\chi(a) \neq 0$. 则对于 a 的任一共轭元 a^x，亦有 $\chi(a^x) \neq 0$，于是由 (1) 有 $a^x \in A$. 令 $N = \langle a^x \bigm| x \in G \rangle$，则 N 即为所求.

20. 设 $\psi \in \mathrm{Irr}(H)$，且 $\psi(1) = b(H)$. 任取 ψ^G 的一个不可约成分 χ，则有 $\langle \chi, \psi^G \rangle_G > 0$，于是又有 $\langle \chi|_H, \psi \rangle_H > 0$，即 ψ 是 $\chi|_H$ 的不可约成分，故 $\chi(1) \geq \psi(1) = b(H)$，因此 $b(G) \geq b(H)$.

设 $\chi \in \mathrm{Irr}(G)$，且 $\chi(1) = b(G)$. 任取 $\chi|_H$ 的一个不可约成分 ψ，则有 $\langle \chi|_H, \psi \rangle_H > 0$，于是又有 $\langle \chi, \psi^H \rangle_G > 0$，即 χ 是 χ^H 的不可约成分. 故 $\chi(1) \leq \psi^H(1) = |G:H|\psi(1) \leq |G:H|b(H)$，因此 $b(G) \leq |G:H| \cdot b(H)$.

22. $\Longrightarrow$: 由 $H \trianglelefteq G$，验证对 H 的任一特征标 φ 均有 $\varphi^G(a) = 0, \forall \in G - H$. 特别地有 χ 在 $G - H$ 上取零值. 现在设 ψ_i 是 $\chi|_H$ 的一个不可约成分. 并设 $\langle \chi|_H, \psi_i \rangle_H = r > 1$. 于是 $\langle \chi, {\psi_i}^H \rangle_G = r > 1$. 特别地，${\psi_i}^H(1) = r\chi(1) > \chi(1) = |G:H|\psi(1)$，于是 $\psi_i(1) > \psi(1)$. 但由 21 题，$\psi_i(1) \leq \psi(1)$，矛盾.

$\Longleftarrow$: 由 χ 在 $G - H$ 上取零值，得

$$1 = \langle \chi, \chi \rangle_G = \frac{1}{|G|} \sum_{a\in G} |\chi(a)|^2 =$$
$$\frac{1}{|G:H|} \cdot \frac{1}{|H|} \cdot \sum_{a\in H} |\chi(a)|^2 = \frac{1}{|G:H|} \langle \chi|_H, \chi|_H \rangle_H,$$

即 $\langle \chi|_H, \chi|_H \rangle_H = |G:H|$. 再设

$$\chi|_H = \psi_1 + \cdots + \psi_m,$$

其中 ψ_i 是 H 的不可约特征标，且 $\psi_1(1) \leq \cdots \leq \psi_m(1)$. 因 $1 = \langle \chi|_H, \psi_1 \rangle_H = \langle \chi, {\psi_1}^H \rangle_G$，有 ${\psi_1}^H(1) \geq \chi(1)$，即 $|G:H| \cdot \psi_1(1) \geq \chi(1)$. 又因 $\psi_1, \cdots, \psi_m$

两两不同，计算 $\langle\chi|_H,\chi|_H\rangle_H$ 可得 $m=|G:H|$，故必有 $\psi_1(1)=\cdots=\psi_m(1)=\frac{1}{|G:H|}\chi(1)$. 由此推出 $\chi={\psi_1}^H=\cdots={\psi_m}^H$.

23. 可设 $\chi(1)=a+b,\chi(t)=a,\forall t\in G$, 其中 a,b 是适当的复常数. 由此有

$$\chi=a1_G+br_G=a1_G+b\sum_{\varphi\in\mathrm{Irr}(G)}\varphi(1)\varphi.$$

因为 χ 是 G 的特征标，易证 a,b 是整数且 $b\geq 0,a+b\geq 0$. 若 $b>0$, 则

$$\chi(1)\geq br_G(1)-b=b(|G|-1)\geq |G|-1.$$

24. 因 $|G|$ 是奇数，对任意的 $1\neq a\in G$, 有 $a\neq a^{-1}$. 令

$$G=\{1,a_1,{a_1}^{-1},a_2,{a_2}^{-1},\cdots,a_m,{a_m}^{-1}\}.$$

则因

$$0=\langle\chi,1_G\rangle_G=\frac{1}{|G|}\left(\chi(1)+\sum_{i=1}^{m}(\chi(a_i)+\chi({a_i}^{-1}))\right),$$

若 $\chi=\overline{\chi}$, 有

$$\chi(1)=-\sum_{i=1}^{m}(\chi(a_i)+\overline{\chi}(a_i))=-2\sum_{i=1}^{m}\chi(a_i).$$

于 $2\mid\chi(1)$. 但 $\chi(1)\mid|G|$, 矛盾.

25. 据 13 题，a 是实元素. 再用 14 题.

26. 设 G 是使结论不真之极小反例. 于是 $A>1$. 取 $1\neq a\in A$, 则 a 所在的共轭类长度为素数方幂，由定理 5.2 推知 G 有非平凡正规子群 N. 考虑 G/N 的交换子群 AN/N. 由 G 的极小性知

$$(G/N)'=G'N/N<G/N,$$

于是 $G'<G$, 矛盾

27. 因 $C_G(P)\not\leq P$, 可取到 p' 子群 $H\leq C_G(P),H\neq 1$. 取 $1\neq h\in H$, 令 $C(h)$ 为 G 中包含 h 的共轭类，则易证 $(|C(h)|,\chi(1))$=1. 由定理 5.1 推知 $\chi(h)=0$ 或 $|\chi(h)|=\chi(1)$. 若对所有的 $1\neq h\in H$, 都有 $\chi(h)=0$, 则 $\chi|_H$ 是 r_H 的整数倍，于是 $\chi(1)$ 是 $|H|$ 的倍数，矛盾. 故存在 $1\neq h\in H$ 使 $|\chi(h)|=\chi(1)$. 设 $\mathbf{X}$ 是 χ 对应的矩阵表示，则 $\mathbf{X}(h)=\varepsilon\mathbf{I}$, ε 是 $|H|$ 次单位根. 因 χ 忠实，$h\neq 1$, 有 $\varepsilon\neq 1$. 考虑 G 的线性表示 $\det\mathbf{X}$, 有 $\det\mathbf{X}(h)=\varepsilon^{\chi(1)}\neq 1$, 即 $\det\mathbf{X}\neq 1_G$. 但若 $G=G'$, G 只有一个线性表示. 即主表示 1_G, 这将导出矛盾.

32. 参看 M. Hall《群论》定理 16.3.1 的第二个证明.

33. 任取 V 的一个 Hermite 内积 f_1, 令

$$f(v_1, v_2) = \sum_{a \in G} f_1(v_1 a, v_2 a), \quad \forall v_1, v_2 \in V.$$

则 f 即满足要求.

34. 取 33 题中的 Hermite 内积, 设 U 是 V 的 G- 子空间, 则 $V = U \oplus U^{\perp}$, 而 $U^{\perp}$ 也是 G- 子空间.

38. 这个问题对偶于定理 3.6(2). 证明时注意我们所谓的模都是有限维的.

42. 用 41 题.

索　引

(以汉语拼音为序)

K

L

M

N

O

P

Y

Z